



Key Management Interoperability Protocol Test Cases Version 1.2

Committee Note 01

11 November 2014

Specification URIs

This version:

<http://docs.oasis-open.org/kmip/testcases/v1.2/cn01/kmip-testcases-v1.2-cn01.doc> (Authoritative)

<http://docs.oasis-open.org/kmip/testcases/v1.2/cn01/kmip-testcases-v1.2-cn01.html>

<http://docs.oasis-open.org/kmip/testcases/v1.2/cn01/kmip-testcases-v1.2-cn01.pdf>

Previous version:

<http://docs.oasis-open.org/kmip/testcases/v1.2/cnprd01/kmip-testcases-v1.2-cnprd01.doc> (Authoritative)

<http://docs.oasis-open.org/kmip/testcases/v1.2/cnprd01/kmip-testcases-v1.2-cnprd01.html>

<http://docs.oasis-open.org/kmip/testcases/v1.2/cnprd01/kmip-testcases-v1.2-cnprd01.pdf>

Latest version:

<http://docs.oasis-open.org/kmip/testcases/v1.2/kmip-testcases-v1.2.doc> (Authoritative)

<http://docs.oasis-open.org/kmip/testcases/v1.2/kmip-testcases-v1.2.html>

<http://docs.oasis-open.org/kmip/testcases/v1.2/kmip-testcases-v1.2.pdf>

Technical Committee:

OASIS Key Management Interoperability Protocol (KMIP) TC

Chairs:

Saikat Saha (saikat.saha@oracle.com), Oracle

Tony Cox (tjc@cryptsoft.com), Cryptsoft Pty Ltd.

Editors:

Tim Hudson (tjh@cryptsoft.com), Cryptsoft Pty Ltd.

Faisal Faruqui (faisal.faruqui@thalessec.com), Thales e-Security

Related work:

This document replaces or supersedes:

This is a Non-Standards
Track Work Product. The
patent provisions of the
OASIS IPR Policy do not
apply.

- *Key Management Interoperability Protocol Test Cases Version 1.1*. Edited by Mathias Björkqvist and Tim Hudson. Latest version. <http://docs.oasis-open.org/kmip/testcases/v1.1/kmip-testcases-v1.1.html>.

This document is related to:

- *Key Management Interoperability Protocol Specification Version 1.2*. Edited by Kiran Thota and Kelley Burgin. Latest version: <http://docs.oasis-open.org/kmip/spec/v1.2/kmip-spec-v1.2.html>.
- *Key Management Interoperability Protocol Profiles Version 1.2*. Edited by Tim Hudson and Robert Lockhart. Latest version: <http://docs.oasis-open.org/kmip/profiles/v1.2/kmip-profiles-v1.2.html>.
- *Key Management Interoperability Protocol Usage Guide Version 1.2*. Edited by Indra Fitzgerald and Judith Furlong. Latest version: <http://docs.oasis-open.org/kmip/ug/v1.2/kmip-ug-v1.2.html>.

Abstract:

This document is intended for developers and architects who wish to design systems and applications that interoperate using the Key Management Interoperability Protocol specification.

Status:

This document was last revised or approved by the OASIS Key Management Interoperability Protocol (KMIP) TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip#technical.

Technical Committee members should send comments on this document to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at <https://www.oasis-open.org/committees/kmip/>.

Citation format:

When referencing this document the following citation format should be used:

[kmip-testcases-v1.2]

Key Management Interoperability Protocol Test Cases Version 1.2. Edited by Tim Hudson and Faisal Faruqui. 11 November 2014. OASIS Committee Note 01. <http://docs.oasis-open.org/kmip/testcases/v1.2/cn01/kmip-testcases-v1.2-cn01.html>. Latest version: <http://docs.oasis-open.org/kmip/testcases/v1.2/kmip-testcases-v1.2.html>.

Copyright © OASIS Open 2014. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full [Policy](#) may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

1	Introduction	8
1.1	References (non-normative).....	8
2	KMIP Test Cases	9
2.1	KMIP 1.0 Test Cases	9
2.1.1	TC-311-10 - Create / Destroy	9
2.1.2	TC-312-10 - Register / Create / Get attributes / Destroy	11
2.1.3	TC-313-10 - Create / Locate / Get / Destroy.....	16
2.1.4	TC-314-10 - Dual Client Test Case, ID Placeholder-linked Locate & Get Batch	20
2.1.5	TC-315-10 - Register / Destroy Secret Data	31
2.1.6	TC-32-10 - Asynchronous Locate	33
2.1.7	TC-41-10 - Revoke Scenario	41
2.1.8	TC-51-10 - Get Usage Allocation Scenario	54
2.1.9	TC-61-10 - Import of a Third-party Key.....	64
2.1.10	TC-71-10 - Unrecognized Message Extension with Criticality Indicator False.....	67
2.1.11	TC-72-10 - Unrecognized Message Extension with Criticality Indicator True.....	69
2.1.12	TC-81-10 - Create a Key Pair	71
2.1.13	TC-82-10 - Register Both Halves of a Key Pair	75
2.1.14	TC-91-10 - Create a Key, Re-key.....	81
2.1.15	TC-92-10 - Existing Key Expired, Re-key with Same Life-cycle.....	87
2.1.16	TC-93-10 - Existing Key Compromised, Re-key with Same Life-cycle	95
2.1.17	TC-94-10 - Create Key, Re-key with New Life-cycle	102
2.1.18	TC-95-10 - Obtain Lease for Expired Key	109
2.1.19	TC-101-10 - Create a Key, Archive and Recover it	118
2.1.20	TC-111-10 - Credential, Operation Policy, Destroy Date	127
2.1.21	TC-121-10 - Query, Maximum Response Size.....	133
2.1.22	TC-131-10 - Register an Asymmetric Key Pair in PKCS1 Format	135
2.1.23	TC-132-10 - Register an Asymmetric Key Pair and a Corresponding X509 Certificate	145
2.1.24	TC-134-10 - Register Key Pair, Certify and Re-certify Public Key	158
2.1.25	TC-NP-1-10 - Put	175
2.1.26	TC-NP-2-10 - Notify & Put.....	179
2.1.27	TC-ECC-1-10 - Register an ECC Key Pair	186
2.1.28	TC-ECC-2-10 - Register an ECC Key Pair in PKCS8 Format.....	194
2.1.29	TC-ECC-3-10 - Register an ECC Key Pair and ECDSA Certificate	203
2.2	KMIP 1.1 Test Cases	216
2.2.1	TC-311-11 - Create / Destroy	216

2.2.2 TC-312-11 - Register / Create / Get attributes / Destroy	218
2.2.3 TC-313-11 - Create / Locate / Get / Destroy	223
2.2.4 TC-314-11 - Dual Client Test Case, ID Placeholder-linked Locate & Get Batch	227
2.2.5 TC-315-11 - Register / Destroy Secret Data	238
2.2.6 TC-32-11 - Asynchronous Locate	240
2.2.7 TC-41-11 - Revoke Scenario	248
2.2.8 TC-51-11 - Get Usage Allocation Scenario	261
2.2.9 TC-61-11 - Import of a Third-party Key	271
2.2.10 TC-71-11 - Unrecognized Message Extension with Criticality Indicator False	275
2.2.11 TC-72-11 - Unrecognized Message Extension with Criticality Indicator True	277
2.2.12 TC-81-11 - Create a Key Pair	278
2.2.13 TC-82-11 - Register Both Halves of a Key Pair	282
2.2.14 TC-91-11 - Create a Key, Re-key	289
2.2.15 TC-92-11 - Existing Key Expired, Re-key with Same Life-cycle	295
2.2.16 TC-93-11 - Existing Key Compromised, Re-key with Same Life-cycle	303
2.2.17 TC-94-11 - Create Key, Re-key with New Life-cycle	309
2.2.18 TC-95-11 - Obtain Lease for Expired Key	316
2.2.19 TC-101-11 - Create a Key, Archive and Recover it	325
2.2.20 TC-111-11 - Credential, Operation Policy, Destroy Date	335
2.2.21 TC-112-11 - Device Credential, Operation Policy, Destroy Date	341
2.2.22 TC-121-11 - Query, Maximum Response Size	348
2.2.23 TC-122-11 - Query Vendor Extensions	350
2.2.24 TC-131-11 - Register an Asymmetric Key Pair in PKCS1 Format	351
2.2.25 TC-132-11 - Register an Asymmetric Key Pair and a Corresponding X509 Certificate	361
2.2.26 TC-133-11 - Create, Re-key Key Pair	375
2.2.27 TC-134-11 - Register Key Pair, Certify and Re-certify Public Key	390
2.2.28 TC-141-11 - Key Wrapping using AES Key Wrap and No Encoding	407
2.2.29 TC-142-11 - Key Wrapping using AES Key Wrap with Attributes	414
2.2.30 TC-151-11 - Locate a Fresh Object from the Default Group	420
2.2.31 TC-152-11 - Client-side Group Management	424
2.2.32 TC-153-11 - Default Object Group Member	433
2.2.33 TC-161-11 - Discover Versions	442
2.2.34 TC-171-11 - Handling of Attributes and Attribute Index Values	445
2.2.35 TC-181-11 - Digests of Symmetric Keys	450
2.2.36 TC-182-11 - Digests of RSA Private Keys	459
2.2.37 TC-NP-1-11 - Put	466
2.2.38 TC-NP-2-11 - Notify & Put	470

2.2.39 TC-ECC-1-11 - Register an ECC Key Pair	478
2.2.40 TC-ECC-2-11 - Register an ECC Key Pair in PKCS8 Format.....	486
2.2.41 TC-ECC-3-11 - Register an ECC Key Pair and ECDSA Certificate	494
2.3 KMIP 1.2 Test Cases.....	508
2.3.1 TC-311-12 - Create / Destroy	508
2.3.2 TC-312-12 - Register / Create / Get attributes / Destroy	510
2.3.3 TC-313-12 - Create / Locate / Get / Destroy.....	519
2.3.4 TC-314-12 - Dual Client Test Case, ID Placeholder-linked Locate & Get Batch	524
2.3.5 TC-315-12 - Register / Destroy Secret Data	536
2.3.6 TC-32-12 - Asynchronous Locate	537
2.3.7 TC-41-12 - Revoke Scenario	545
2.3.8 TC-51-12 - Get Usage Allocation Scenario	559
2.3.9 TC-61-12 - Import of a Third-party Key.....	569
2.3.10 TC-71-12 - Unrecognized Message Extension with Criticality Indicator False.....	572
2.3.11 TC-72-12 - Unrecognized Message Extension with Criticality Indicator True.....	574
2.3.12 TC-81-12 - Create a Key Pair	576
2.3.13 TC-82-12 - Register Both Halves of a Key Pair	580
2.3.14 TC-91-12 - Create a Key, Re-key.....	586
2.3.15 TC-92-12 - Existing Key Expired, Re-key with Same Life-cycle.....	592
2.3.16 TC-93-12 - Existing Key Compromised, Re-key with Same Life-cycle	600
2.3.17 TC-94-12 - Create Key, Re-key with New Life-cycle	607
2.3.18 TC-95-12 - Obtain Lease for Expired Key	614
2.3.19 TC-101-12 - Create a Key, Archive and Recover it	622
2.3.20 TC-111-12 - Credential, Operation Policy, Destroy Date	633
2.3.21 TC-112-12 - Device Credential, Operation Policy, Destroy Date	639
2.3.22 TC-121-12 - Query, Maximum Response Size.....	645
2.3.23 TC-122-12 - Query Vendor Extensions.....	648
2.3.24 TC-131-12 - Register an Asymmetric Key Pair in PKCS1 Format.....	649
2.3.25 TC-132-12 - Register an Asymmetric Key Pair and a Corresponding X509 Certificate	659
2.3.26 TC-133-12 - Create, Re-key Key Pair	673
2.3.27 TC-134-12 - Register Key Pair, Certify and Re-certify Public Key	688
2.3.28 TC-141-12 - Key Wrapping using AES Key Wrap and No Encoding.....	705
2.3.29 TC-142-12 - Key Wrapping using AES Key Wrap with Attributes.....	712
2.3.30 TC-151-12 - Locate a Fresh Object from the Default Group.....	718
2.3.31 TC-152-12 - Client-side Group Management.....	722
2.3.32 TC-153-12 - Default Object Group Member	731
2.3.33 TC-161-12 - Discover Versions	740

2.3.34 TC-171-12 - Handling of Attributes and Attribute Index Values.....	744
2.3.35 TC-181-12 - Digests of Symmetric Keys	749
2.3.36 TC-182-12 - Digests of RSA Private Keys	758
2.3.37 TC-NP-1-12 - Put	765
2.3.38 TC-NP-2-12 - Notify & Put	769
2.3.39 TC-ECC-1-12 - Register an ECC Key Pair	777
2.3.40 TC-ECC-2-12 - Register an ECC Key Pair in PKCS8 Format.....	785
2.3.41 TC-ECC-3-12 - Register an ECC Key Pair and ECDSA Certificate	793
2.3.42 TC-PGP-1-12 - Register PGP Key - RSA	807
2.3.43 TC-MDO-1-12 - Register MDO Key.....	820
2.3.44 TC-MDO-2-12 - Locate MDO keys by Key Value Present	824
2.3.45 TC-MDO-3-12 - Register MDO Key using PKCS11 URI.....	830
2.3.46 TC-SJ-1-12 - Create and Split/Join.....	834
2.3.47 TC-SJ-2-12 - Register and Split / Join	843
2.3.48 TC-SJ-3-12 - Join Split Keys.....	855
2.3.49 TC-SJ-4-12 - Register and Split / Join with XOR.....	864
Appendix A. Acknowledgments	877
Appendix B. Revision History	880

1 Introduction

The purpose of this document is to describe test cases to demonstrate the Key Management Interoperability Protocol (KMIP) [KMIP-SPEC-1_2], [KMIP-SPEC-1_1], and [KMIP-SPEC-1_0]. The test cases illustrate that the concepts within the protocol are sound and how the protocol may be used when implementing KMIP in applications. These test cases are not intended to fully test an implementation of KMIP. There are test cases for v1.0, v1.1 and v1.2 of the protocol.

1.1 References (non-normative)

[KMIP-SPEC-1_0]

Key Management Interoperability Protocol Specification Version 1.0. October 2010. OASIS Standard. <http://docs.oasis-open.org/kmip/spec/v1.0/os/kmip-spec-1.0-os.doc>.

[KMIP-SPEC-1_1]

Key Management Interoperability Protocol Specification Version 1.1. 24 January 2013. OASIS Standard. <http://docs.oasis-open.org/kmip/spec/v1.1/os/kmip-spec-v1.1-os.doc>.

[KMIP-SPEC-1_2]

Key Management Interoperability Protocol Specification Version 1.2. Edited by Kiran Thota and Kelley Burgin. Latest version: <http://docs.oasis-open.org/kmip/spec/v1.2/kmip-spec-v1.2.doc>.

[KMIP-ENCODINGS]

KMIP Additional Message Encodings Version 1.0. Edited by Tim Hudson. Latest version: <http://docs.oasis-open.org/kmip/kmip-addtl-msg-enc/v1.0/kmip-addtl-msg-enc-v1.0.doc>.

2 KMIP Test Cases

The test cases define a number of request-response pairs for KMIP operations. Each test case is provided in the XML format specified in [KMIP-ENCODINGS] intended to be both human-readable and usable by automated tools. The time sequence (starting from 0) for each request-response pair is noted and line numbers are provided for ease of cross-reference for a given test sequence.

Each test case has a unique label (the section name) which includes the protocol version as part of the identifier.

Many of the test cases contained within this document depend on a specific configuration of a KMIP server to match the assumptions of the test case. Support for a test case depends on a server being configured in a manner consistent with the test case assumptions.

The test cases show one possible way to construct the messages, and the messages shown are not necessarily the only conformant constructions as many items within KMIP are optional and server behavior depends on the server's policy. Support for a test case is predicated on a server matching the test case assumptions and the behavior shown in the request-response pairs.

Where possible the flow of unique identifiers between tests, the date-time values, and other dynamic items are indicated using symbolic identifiers – in actual request and response messages these dynamic values will be filled in with valid values.

2.1 KMIP 1.0 Test Cases

2.1.1 TC-311-10 - Create / Destroy

In this test case the client issues a Create request, whereby the server creates a new symmetric key and returns the Unique Identifier. To clean up, the client then performs a Destroy operation to destroy the key.

```
# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="0"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="Create"/>
0011     <RequestPayload>
0012       <ObjectType type="Enumeration" value="SymmetricKey"/>
0013       <TemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
```

0016	<AttributeValue type="Enumeration" value="AES"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	</TemplateAttribute>
0027	</RequestPayload>
0028	</BatchItem>
0029	</RequestMessage>
0030	<ResponseMessage>
0031	<ResponseHeader>
0032	<ProtocolVersion>
0033	<ProtocolVersionMajor type="Integer" value="1"/>
0034	<ProtocolVersionMinor type="Integer" value="0"/>
0035	</ProtocolVersion>
0036	<TimeStamp type="DateTime" value="2009-11-12T10:47:30+00:00"/>
0037	<BatchCount type="Integer" value="1"/>
0038	</ResponseHeader>
0039	<BatchItem>
0040	<Operation type="Enumeration" value="Create"/>
0041	<ResultStatus type="Enumeration" value="Success"/>
0042	<ResponsePayload>
0043	<ObjectType type="Enumeration" value="SymmetricKey"/>
0044	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0045	</ResponsePayload>
0046	</BatchItem>
0047	</ResponseMessage>
0048	# TIME 1 <RequestMessage>
0049	<RequestHeader>
0050	<ProtocolVersion>
0051	<ProtocolVersionMajor type="Integer" value="1"/>
0052	<ProtocolVersionMinor type="Integer" value="0"/>
0053	</ProtocolVersion>
0054	<BatchCount type="Integer" value="1"/>
0055	</RequestHeader>
0056	<BatchItem>
0057	<Operation type="Enumeration" value="Destroy"/>
0058	<RequestPayload>
0059	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0060	</RequestPayload>
0061	</BatchItem>
0062	</RequestMessage>
0063	<ResponseMessage>
0064	<ResponseHeader>
0065	<ProtocolVersion>
0066	<ProtocolVersionMajor type="Integer" value="1"/>

```

0067     <ProtocolVersionMinor type="Integer" value="0"/>
0068     </ProtocolVersion>
0069     <TimeStamp type="DateTime" value="2009-11-12T10:47:31+00:00"/>
0070     <BatchCount type="Integer" value="1"/>
0071 </ResponseHeader>
0072 <BatchItem>
0073     <Operation type="Enumeration" value="Destroy"/>
0074     <ResultStatus type="Enumeration" value="Success"/>
0075     <ResponsePayload>
0076         <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0077     </ResponsePayload>
0078 </BatchItem>
0079 </ResponseMessage>

```

46

47 2.1.2 TC-312-10 - Register / Create / Get attributes / Destroy

48 Here the client first registers a template object and then creates a symmetric key using the
49 registered template. To verify that the attributes of the key were set correctly from the
50 template, the client then issues a Get Attributes command, after which it destroys first the key
51 and then the template.

```

# TIME 0
0001 <RequestMessage>
0002 <RequestHeader>
0003     <ProtocolVersion>
0004         <ProtocolVersionMajor type="Integer" value="1"/>
0005         <ProtocolVersionMinor type="Integer" value="0"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008 </RequestHeader>
0009 <BatchItem>
0010     <Operation type="Enumeration" value="Register"/>
0011     <RequestPayload>
0012         <ObjectType type="Enumeration" value="Template"/>
0013         <TemplateAttribute>
0014             </TemplateAttribute>
0015         <Template>
0016             <Attribute>
0017                 <AttributeName type="TextString" value="Object Group"/>
0018                 <AttributeValue type="TextString" value="Group1"/>
0019             </Attribute>
0020             <Attribute>
0021                 <AttributeName type="TextString" value="Application
Specific Information"/>
0022                 <AttributeValue>
0023                     <ApplicationNamespace type="TextString" value="ssl"/>
0024                     <ApplicationData type="TextString"
value="www.example.com"/>
0025                 </AttributeValue>
0026             </Attribute>
0027             <Attribute>
0028                 <AttributeName type="TextString" value="Contact
Information"/>

```

0029	<AttributeValue type="TextString" value="Joe"/>
0030	</Attribute>
0031	<Attribute>
0032	<AttributeName type="TextString" value="x-Purpose"/>
0033	<AttributeValue type="TextString" value="demonstration"/>
0034	</Attribute>
0035	<Attribute>
0036	<AttributeName type="TextString" value="Name"/>
0037	<AttributeValue>
0038	<NameValue type="TextString" value="Template1"/>
0039	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0040	</AttributeValue>
0041	</Attribute>
0042	</Template>
0043	</RequestPayload>
0044	</BatchItem>
0045	</RequestMessage>
0046	<ResponseMessage>
0047	<ResponseHeader>
0048	<ProtocolVersion>
0049	<ProtocolVersionMajor type="Integer" value="1"/>
0050	<ProtocolVersionMinor type="Integer" value="0"/>
0051	</ProtocolVersion>
0052	<TimeStamp type="DateTime" value="2009-11-12T10:47:32+00:00"/>
0053	<BatchCount type="Integer" value="1"/>
0054	</ResponseHeader>
0055	<BatchItem>
0056	<Operation type="Enumeration" value="Register"/>
0057	<ResultStatus type="Enumeration" value="Success"/>
0058	<ResponsePayload>
0059	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0060	</ResponsePayload>
0061	</BatchItem>
0062	</ResponseMessage>
	# TIME 1
0063	<RequestMessage>
0064	<RequestHeader>
0065	<ProtocolVersion>
0066	<ProtocolVersionMajor type="Integer" value="1"/>
0067	<ProtocolVersionMinor type="Integer" value="0"/>
0068	</ProtocolVersion>
0069	<BatchCount type="Integer" value="1"/>
0070	</RequestHeader>
0071	<BatchItem>
0072	<Operation type="Enumeration" value="Create"/>
0073	<RequestPayload>
0074	<ObjectType type="Enumeration" value="SymmetricKey"/>
0075	<TemplateAttribute>
0076	<Name>
0077	<NameValue type="TextString" value="Template1"/>
0078	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0079	</Name>
0080	<Attribute>
0081	<AttributeName type="TextString" value="Cryptographic

0082	Algorithm"/>
0083	<AttributeValue type="Enumeration" value="AES"/>
0084	</Attribute>
0085	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0086	<AttributeValue type="Integer" value="128"/>
0087	</Attribute>
0088	<Attribute>
0089	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0090	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0091	</Attribute>
0092	</TemplateAttribute>
0093	</RequestPayload>
0094	</BatchItem>
0095	</RequestMessage>
0096	<ResponseMessage>
0097	<ResponseHeader>
0098	<ProtocolVersion>
0099	<ProtocolVersionMajor type="Integer" value="1"/>
0100	<ProtocolVersionMinor type="Integer" value="0"/>
0101	</ProtocolVersion>
0102	<TimeStamp type="DateTime" value="2009-11-12T10:47:33+00:00"/>
0103	<BatchCount type="Integer" value="1"/>
0104	</ResponseHeader>
0105	<BatchItem>
0106	<Operation type="Enumeration" value="Create"/>
0107	<ResultStatus type="Enumeration" value="Success"/>
0108	<ResponsePayload>
0109	<ObjectType type="Enumeration" value="SymmetricKey"/>
0110	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0111	</ResponsePayload>
0112	</BatchItem>
0113	</ResponseMessage>
	# TIME 2
0114	<RequestMessage>
0115	<RequestHeader>
0116	<ProtocolVersion>
0117	<ProtocolVersionMajor type="Integer" value="1"/>
0118	<ProtocolVersionMinor type="Integer" value="0"/>
0119	</ProtocolVersion>
0120	<BatchCount type="Integer" value="1"/>
0121	</RequestHeader>
0122	<BatchItem>
0123	<Operation type="Enumeration" value="GetAttributes"/>
0124	<RequestPayload>
0125	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0126	<AttributeName type="TextString" value="Object Group"/>
0127	<AttributeName type="TextString" value="Application Specific
	Information"/>
0128	<AttributeName type="TextString" value="Contact Information"/>
0129	<AttributeName type="TextString" value="x-Purpose"/>
0130	</RequestPayload>
0131	</BatchItem>

0132	</RequestMessage>
0133	<ResponseMessage>
0134	<ResponseHeader>
0135	<ProtocolVersion>
0136	<ProtocolVersionMajor type="Integer" value="1"/>
0137	<ProtocolVersionMinor type="Integer" value="0"/>
0138	</ProtocolVersion>
0139	<TimeStamp type="DateTime" value="2009-11-12T10:47:34+00:00"/>
0140	<BatchCount type="Integer" value="1"/>
0141	</ResponseHeader>
0142	<BatchItem>
0143	<Operation type="Enumeration" value="GetAttributes"/>
0144	<ResultStatus type="Enumeration" value="Success"/>
0145	<ResponsePayload>
0146	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0147	<Attribute>
0148	<AttributeName type="TextString" value="Object Group"/>
0149	<AttributeValue type="TextString" value="Group1"/>
0150	</Attribute>
0151	<Attribute>
0152	<AttributeName type="TextString" value="Application Specific
	Information"/>
0153	<AttributeValue>
0154	<ApplicationNamespace type="TextString" value="ssl"/>
0155	<ApplicationData type="TextString"
	value="www.example.com"/>
0156	</AttributeValue>
0157	</Attribute>
0158	<Attribute>
0159	<AttributeName type="TextString" value="Contact
	Information"/>
0160	<AttributeValue type="TextString" value="Joe"/>
0161	</Attribute>
0162	<Attribute>
0163	<AttributeName type="TextString" value="x-Purpose"/>
0164	<AttributeValue type="TextString" value="demonstration"/>
0165	</Attribute>
0166	</ResponsePayload>
0167	</BatchItem>
0168	</ResponseMessage>
	# TIME 3
0169	<RequestMessage>
0170	<RequestHeader>
0171	<ProtocolVersion>
0172	<ProtocolVersionMajor type="Integer" value="1"/>
0173	<ProtocolVersionMinor type="Integer" value="0"/>
0174	</ProtocolVersion>
0175	<BatchCount type="Integer" value="1"/>
0176	</RequestHeader>
0177	<BatchItem>
0178	<Operation type="Enumeration" value="Destroy"/>
0179	<RequestPayload>
0180	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0181	</RequestPayload>
0182	</BatchItem>

0183	</RequestMessage>
0184	<ResponseMessage>
0185	<ResponseHeader>
0186	<ProtocolVersion>
0187	<ProtocolVersionMajor type="Integer" value="1"/>
0188	<ProtocolVersionMinor type="Integer" value="0"/>
0189	</ProtocolVersion>
0190	<TimeStamp type="DateTime" value="2009-11-12T10:47:34+00:00"/>
0191	<BatchCount type="Integer" value="1"/>
0192	</ResponseHeader>
0193	<BatchItem>
0194	<Operation type="Enumeration" value="Destroy"/>
0195	<ResultStatus type="Enumeration" value="Success"/>
0196	<ResponsePayload>
0197	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0198	</ResponsePayload>
0199	</BatchItem>
0200	</ResponseMessage>
# TIME 4	
0201	<RequestMessage>
0202	<RequestHeader>
0203	<ProtocolVersion>
0204	<ProtocolVersionMajor type="Integer" value="1"/>
0205	<ProtocolVersionMinor type="Integer" value="0"/>
0206	</ProtocolVersion>
0207	<BatchCount type="Integer" value="1"/>
0208	</RequestHeader>
0209	<BatchItem>
0210	<Operation type="Enumeration" value="Destroy"/>
0211	<RequestPayload>
0212	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0213	</RequestPayload>
0214	</BatchItem>
0215	</RequestMessage>
0216	<ResponseMessage>
0217	<ResponseHeader>
0218	<ProtocolVersion>
0219	<ProtocolVersionMajor type="Integer" value="1"/>
0220	<ProtocolVersionMinor type="Integer" value="0"/>
0221	</ProtocolVersion>
0222	<TimeStamp type="DateTime" value="2009-11-12T10:47:34+00:00"/>
0223	<BatchCount type="Integer" value="1"/>
0224	</ResponseHeader>
0225	<BatchItem>
0226	<Operation type="Enumeration" value="Destroy"/>
0227	<ResultStatus type="Enumeration" value="Success"/>
0228	<ResponsePayload>
0229	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0230	</ResponsePayload>
0231	</BatchItem>
0232	</ResponseMessage>

53 2.1.3 TC-313-10 - Create / Locate / Get / Destroy

54 This test case tests the Locate and Get operations, in addition to the previously used operations
55 Create and Destroy. A symmetric key is first created, and then a lookup is performed on the
56 Name attribute using the Locate operation. Subsequently, a Get request is issued to retrieve the
57 located key, after which the key on the server is destroyed.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Name"/>
0016	<AttributeValue>
0017	<NameValue type="TextString" value="Key1"/>
0018	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0019	</AttributeValue>
0020	</Attribute>
0021	<Attribute>
0022	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0023	<AttributeValue type="Enumeration" value="DES3"/>
0024	</Attribute>
0025	<Attribute>
0026	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0027	<AttributeValue type="Integer" value="168"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0031	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0032	</Attribute>
0033	<Attribute>
0034	<AttributeName type="TextString" value="Contact
	Information"/>
0035	<AttributeValue type="TextString" value="Joe"/>
0036	</Attribute>
0037	</TemplateAttribute>
0038	</RequestPayload>
0039	</BatchItem>
0040	</RequestMessage>
0041	<ResponseMessage>
0042	<ResponseHeader>
0043	<ProtocolVersion>

0044	<ProtocolVersionMajor type="Integer" value="1"/>
0045	<ProtocolVersionMinor type="Integer" value="0"/>
0046	</ProtocolVersion>
0047	<TimeStamp type="DateTime" value="2009-11-12T10:47:35+00:00"/>
0048	<BatchCount type="Integer" value="1"/>
0049	</ResponseHeader>
0050	<BatchItem>
0051	<Operation type="Enumeration" value="Create"/>
0052	<ResultStatus type="Enumeration" value="Success"/>
0053	<ResponsePayload>
0054	<ObjectType type="Enumeration" value="SymmetricKey"/>
0055	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0056	</ResponsePayload>
0057	</BatchItem>
0058	</ResponseMessage>
	# TIME 1
0059	<RequestMessage>
0060	<RequestHeader>
0061	<ProtocolVersion>
0062	<ProtocolVersionMajor type="Integer" value="1"/>
0063	<ProtocolVersionMinor type="Integer" value="0"/>
0064	</ProtocolVersion>
0065	<BatchCount type="Integer" value="1"/>
0066	</RequestHeader>
0067	<BatchItem>
0068	<Operation type="Enumeration" value="Locate"/>
0069	<RequestPayload>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Object Type"/>
0072	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0073	</Attribute>
0074	<Attribute>
0075	<AttributeName type="TextString" value="Name"/>
0076	<AttributeValue>
0077	<NameValue type="TextString" value="Key1"/>
0078	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0079	</AttributeValue>
0080	</Attribute>
0081	</RequestPayload>
0082	</BatchItem>
0083	</RequestMessage>
0084	<ResponseMessage>
0085	<ResponseHeader>
0086	<ProtocolVersion>
0087	<ProtocolVersionMajor type="Integer" value="1"/>
0088	<ProtocolVersionMinor type="Integer" value="0"/>
0089	</ProtocolVersion>
0090	<TimeStamp type="DateTime" value="2009-11-12T10:47:36+00:00"/>
0091	<BatchCount type="Integer" value="1"/>
0092	</ResponseHeader>
0093	<BatchItem>
0094	<Operation type="Enumeration" value="Locate"/>
0095	<ResultStatus type="Enumeration" value="Success"/>
0096	<ResponsePayload>
0097	<UniqueIdentifier type="TextString"

0098	value="\$UNIQUE_IDENTIFIER_0"/>
0099	</ResponsePayload>
0100	</BatchItem>
	</ResponseMessage>
0101	# TIME 2
0102	<RequestMessage>
0103	<RequestHeader>
0104	<ProtocolVersion>
0105	<ProtocolVersionMajor type="Integer" value="1"/>
0106	<ProtocolVersionMinor type="Integer" value="0"/>
0107	</ProtocolVersion>
0108	<BatchCount type="Integer" value="1"/>
0109	</BatchItem>
0110	<Operation type="Enumeration" value="Get"/>
0111	<RequestPayload>
0112	<UniqueIdentifier type="TextString"
0113	value="\$UNIQUE_IDENTIFIER_0"/>
0114	</RequestPayload>
0115	</BatchItem>
0116	</RequestMessage>
0117	<ResponseMessage>
0118	<ResponseHeader>
0119	<ProtocolVersion>
0120	<ProtocolVersionMajor type="Integer" value="1"/>
0121	<ProtocolVersionMinor type="Integer" value="0"/>
0122	</ProtocolVersion>
0123	<TimeStamp type="DateTime" value="2009-11-12T10:47:36+00:00"/>
0124	<BatchCount type="Integer" value="1"/>
0125	</ResponseHeader>
0126	<BatchItem>
0127	<Operation type="Enumeration" value="Get"/>
0128	<ResultStatus type="Enumeration" value="Success"/>
0129	<ResponsePayload>
0130	<ObjectType type="Enumeration" value="SymmetricKey"/>
0131	<UniqueIdentifier type="TextString"
0132	value="\$UNIQUE_IDENTIFIER_0"/>
0133	<SymmetricKey>
0134	<KeyBlock>
0135	<KeyFormatType type="Enumeration" value="Raw"/>
0136	<KeyValue>
0137	<KeyMaterial type="ByteString"
0138	value="c8e51523f73d6ee9f40eab7cd06825499d8c0bd0739e1046"/>
0139	</KeyValue>
0140	<CryptographicAlgorithm type="Enumeration" value="DES3"/>
0141	<CryptographicLength type="Integer" value="168"/>
0142	</KeyBlock>
0143	</SymmetricKey>
0144	</ResponsePayload>
0145	</BatchItem>
0146	</ResponseMessage>
0147	# TIME 3
	<RequestMessage>
	<RequestHeader>
	<ProtocolVersion>
	<ProtocolVersionMajor type="Integer" value="1"/>

0148	<ProtocolVersionMinor type="Integer" value="0"/>
0149	</ProtocolVersion>
0150	<BatchCount type="Integer" value="1"/>
0151	</RequestHeader>
0152	<BatchItem>
0153	<Operation type="Enumeration" value="Destroy"/>
0154	<RequestPayload>
0155	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0156	</RequestPayload>
0157	</BatchItem>
0158	</RequestMessage>
0159	<ResponseMessage>
0160	<ResponseHeader>
0161	<ProtocolVersion>
0162	<ProtocolVersionMajor type="Integer" value="1"/>
0163	<ProtocolVersionMinor type="Integer" value="0"/>
0164	</ProtocolVersion>
0165	<TimeStamp type="DateTime" value="2009-11-12T10:47:36+00:00"/>
0166	<BatchCount type="Integer" value="1"/>
0167	</ResponseHeader>
0168	<BatchItem>
0169	<Operation type="Enumeration" value="Destroy"/>
0170	<ResultStatus type="Enumeration" value="Success"/>
0171	<ResponsePayload>
0172	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0173	</ResponsePayload>
0174	</BatchItem>
0175	</ResponseMessage>
	# TIME 4
0176	<RequestMessage>
0177	<RequestHeader>
0178	<ProtocolVersion>
0179	<ProtocolVersionMajor type="Integer" value="1"/>
0180	<ProtocolVersionMinor type="Integer" value="0"/>
0181	</ProtocolVersion>
0182	<BatchCount type="Integer" value="1"/>
0183	</RequestHeader>
0184	<BatchItem>
0185	<Operation type="Enumeration" value="Locate"/>
0186	<RequestPayload>
0187	<Attribute>
0188	<AttributeName type="TextString" value="Unique Identifier"/>
0189	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0190	</Attribute>
0191	</RequestPayload>
0192	</BatchItem>
0193	</RequestMessage>
0194	<ResponseMessage>
0195	<ResponseHeader>
0196	<ProtocolVersion>
0197	<ProtocolVersionMajor type="Integer" value="1"/>
0198	<ProtocolVersionMinor type="Integer" value="0"/>
0199	</ProtocolVersion>

```
0200     <TimeStamp type="DateTime" value="2009-11-12T10:47:36+00:00"/>
0201     <BatchCount type="Integer" value="1"/>
0202   </ResponseHeader>
0203   <BatchItem>
0204     <Operation type="Enumeration" value="Locate"/>
0205     <ResultStatus type="Enumeration" value="Success"/>
0206     <ResponsePayload>
0207   </ResponsePayload>
0208   </BatchItem>
0209 </ResponseMessage>
```

58

59 2.1.4 TC-314-10 - Dual Client Test Case, ID Placeholder-linked Locate & Get 60 Batch

61 This test case has two clients performing operations on the same key. The first client initially
62 registers a template and creates a symmetric key using that template. The second client then
63 does a batched Locate and Get using the ID Placeholder to retrieve the key. The second client
64 thereafter performs a number of operations on the key (Get Attribute List, Get Attribute, Add
65 Attribute, Modify Attribute and Delete Attribute), before the first client finally destroys the key
66 and the template. The first client also tries to Get the key and the template after they have been
67 destroyed, but the Get operation fails in both cases. This test case demonstrates the fact that it
68 is possible for two clients to cooperate and use the same managed object while only having
69 knowledge of a single pre-agreed Name attribute value and without having to share any other
70 information.

```
0001 # TIME 0
0002 <RequestMessage>
0003   <RequestHeader>
0004     <ProtocolVersion>
0005       <ProtocolVersionMajor type="Integer" value="1"/>
0006       <ProtocolVersionMinor type="Integer" value="0"/>
0007     </ProtocolVersion>
0008     <BatchCount type="Integer" value="1"/>
0009   </RequestHeader>
0010   <BatchItem>
0011     <Operation type="Enumeration" value="Register"/>
0012     <RequestPayload>
0013       <ObjectType type="Enumeration" value="Template"/>
0014       <TemplateAttribute>
0015         </TemplateAttribute>
0016         <Template>
0017           <Attribute>
0018             <AttributeName type="TextString" value="Cryptographic
0019 Algorithm"/>
0020             <AttributeValue type="Enumeration" value="AES"/>
0021           </Attribute>
0022           <Attribute>
0023             <AttributeName type="TextString" value="Cryptographic
0024 Length"/>
0025             <AttributeValue type="Integer" value="128"/>
0026           </Attribute>
0027         </Template>
0028       </TemplateAttribute>
0029     </RequestPayload>
0030   </BatchItem>
0031 </RequestMessage>
```

0025	<AttributeName type="TextString" value="Name"/>
0026	<AttributeValue>
0027	<NameValue type="TextString" value="Templatel"/>
0028	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0029	</AttributeValue>
0030	</Attribute>
0031	</Template>
0032	</RequestPayload>
0033	</BatchItem>
0034	</RequestMessage>
0035	<ResponseMessage>
0036	<ResponseHeader>
0037	<ProtocolVersion>
0038	<ProtocolVersionMajor type="Integer" value="1"/>
0039	<ProtocolVersionMinor type="Integer" value="0"/>
0040	</ProtocolVersion>
0041	<TimeStamp type="DateTime" value="2009-11-12T11:10:25+00:00"/>
0042	<BatchCount type="Integer" value="1"/>
0043	</ResponseHeader>
0044	<BatchItem>
0045	<Operation type="Enumeration" value="Register"/>
0046	<ResultStatus type="Enumeration" value="Success"/>
0047	<ResponsePayload>
0048	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0049	</ResponsePayload>
0050	</BatchItem>
0051	</ResponseMessage>
	# TIME 1
0052	<RequestMessage>
0053	<RequestHeader>
0054	<ProtocolVersion>
0055	<ProtocolVersionMajor type="Integer" value="1"/>
0056	<ProtocolVersionMinor type="Integer" value="0"/>
0057	</ProtocolVersion>
0058	<BatchCount type="Integer" value="1"/>
0059	</RequestHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="Create"/>
0062	<RequestPayload>
0063	<ObjectType type="Enumeration" value="SymmetricKey"/>
0064	<TemplateAttribute>
0065	<Name>
0066	<NameValue type="TextString" value="Templatel"/>
0067	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0068	</Name>
0069	<Attribute>
0070	<AttributeName type="TextString" value="Name"/>
0071	<AttributeValue>
0072	<NameValue type="TextString" value="Key1"/>
0073	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0074	</AttributeValue>
0075	</Attribute>
0076	<Attribute>

0077	<AttributeName type="TextString" value="Cryptographic
0078	Usage Mask"/>
0079	<AttributeValue type="Integer" value="Encrypt"/>
0080	</Attribute>
0081	<AttributeName type="TextString" value="Contact
0082	Information"/>
0083	<AttributeValue type="TextString" value="Foo"/>
0084	</Attribute>
0085	</TemplateAttribute>
0086	</RequestPayload>
0087	</BatchItem>
0088	</RequestMessage>
0089	<ResponseMessage>
0090	<ResponseHeader>
0091	<ProtocolVersion>
0092	<ProtocolVersionMajor type="Integer" value="1"/>
0093	<ProtocolVersionMinor type="Integer" value="0"/>
0094	</ProtocolVersion>
0095	<TimeStamp type="DateTime" value="2009-11-12T11:10:27+00:00"/>
0096	<BatchCount type="Integer" value="1"/>
0097	</ResponseHeader>
0098	<BatchItem>
0099	<Operation type="Enumeration" value="Create"/>
0100	<ResultStatus type="Enumeration" value="Success"/>
0101	<ResponsePayload>
0102	<ObjectType type="Enumeration" value="SymmetricKey"/>
0103	<UniqueIdentifier type="TextString"
0104	value="\$UNIQUE_IDENTIFIER_1"/>
0105	</ResponsePayload>
0106	</BatchItem>
0107	</ResponseMessage>
0108	# TIME 2
0109	<RequestMessage>
0110	<RequestHeader>
0111	<ProtocolVersion>
0112	<ProtocolVersionMajor type="Integer" value="1"/>
0113	<ProtocolVersionMinor type="Integer" value="0"/>
0114	</ProtocolVersion>
0115	<BatchOrderOption type="Boolean" value="true"/>
0116	<BatchCount type="Integer" value="2"/>
0117	</RequestHeader>
0118	<BatchItem>
0119	<Operation type="Enumeration" value="Locate"/>
0120	<UniqueBatchItemID type="ByteString" value="0e9e1875336e415e"/>
0121	<RequestPayload>
0122	<Attribute>
0123	<AttributeName type="TextString" value="Object Type"/>
0124	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0125	</Attribute>
0126	<Attribute>
0127	<AttributeName type="TextString" value="Name"/>
0128	<AttributeValue>
	<NameValue type="TextString" value="Key1"/>
	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
	</AttributeValue>

0129	</Attribute>
0130	</RequestPayload>
0131	</BatchItem>
0132	<BatchItem>
0133	<Operation type="Enumeration" value="Get"/>
0134	<UniqueBatchItemID type="ByteString" value="cfef21dddf1cf5e3"/>
0135	<RequestPayload>
0136	</RequestPayload>
0137	</BatchItem>
0138	</RequestMessage>
0139	<ResponseMessage>
0140	<ResponseHeader>
0141	<ProtocolVersion>
0142	<ProtocolVersionMajor type="Integer" value="1"/>
0143	<ProtocolVersionMinor type="Integer" value="0"/>
0144	</ProtocolVersion>
0145	<TimeStamp type="DateTime" value="2009-11-12T11:10:28+00:00"/>
0146	<BatchCount type="Integer" value="2"/>
0147	</ResponseHeader>
0148	<BatchItem>
0149	<Operation type="Enumeration" value="Locate"/>
0150	<UniqueBatchItemID type="ByteString" value="0e9e1875336e415e"/>
0151	<ResultStatus type="Enumeration" value="Success"/>
0152	<ResponsePayload>
0153	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0154	</ResponsePayload>
0155	</BatchItem>
0156	<BatchItem>
0157	<Operation type="Enumeration" value="Get"/>
0158	<UniqueBatchItemID type="ByteString" value="cfef21dddf1cf5e3"/>
0159	<ResultStatus type="Enumeration" value="Success"/>
0160	<ResponsePayload>
0161	<ObjectType type="Enumeration" value="SymmetricKey"/>
0162	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0163	<SymmetricKey>
0164	<KeyBlock>
0165	<KeyFormatType type="Enumeration" value="Raw"/>
0166	<KeyValue>
0167	<KeyMaterial type="ByteString" value="755d03c639648fb5828d5f1cc9fe9b57"/>
0168	</KeyValue>
0169	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0170	<CryptographicLength type="Integer" value="128"/>
0171	</KeyBlock>
0172	</SymmetricKey>
0173	</ResponsePayload>
0174	</BatchItem>
0175	</ResponseMessage>
# TIME 3	
0176	<RequestMessage>
0177	<RequestHeader>
0178	<ProtocolVersion>
0179	<ProtocolVersionMajor type="Integer" value="1"/>
0180	<ProtocolVersionMinor type="Integer" value="0"/>
0181	</ProtocolVersion>

0182	<BatchCount type="Integer" value="1"/>
0183	</RequestHeader>
0184	<BatchItem>
0185	<Operation type="Enumeration" value="GetAttributeList"/>
0186	<RequestPayload>
0187	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0188	</RequestPayload>
0189	</BatchItem>
0190	</RequestMessage>
0191	<ResponseMessage>
0192	<ResponseHeader>
0193	<ProtocolVersion>
0194	<ProtocolVersionMajor type="Integer" value="1"/>
0195	<ProtocolVersionMinor type="Integer" value="0"/>
0196	</ProtocolVersion>
0197	<TimeStamp type="DateTime" value="2009-11-12T11:10:28+00:00"/>
0198	<BatchCount type="Integer" value="1"/>
0199	</ResponseHeader>
0200	<BatchItem>
0201	<Operation type="Enumeration" value="GetAttributeList"/>
0202	<ResultStatus type="Enumeration" value="Success"/>
0203	<ResponsePayload>
0204	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0205	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0206	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0207	<AttributeName type="TextString" value="State"/>
0208	<AttributeName type="TextString" value="Digest"/>
0209	<AttributeName type="TextString" value="Initial Date"/>
0210	<AttributeName type="TextString" value="Unique Identifier"/>
0211	<AttributeName type="TextString" value="Name"/>
0212	<AttributeName type="TextString" value="Lease Time"/>
0213	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0214	<AttributeName type="TextString" value="Object Type"/>
0215	<AttributeName type="TextString" value="Contact Information"/>
0216	<AttributeName type="TextString" value="Last Change Date"/>
0217	</ResponsePayload>
0218	</BatchItem>
0219	</ResponseMessage>
	# TIME 4
0220	<RequestMessage>
0221	<RequestHeader>
0222	<ProtocolVersion>
0223	<ProtocolVersionMajor type="Integer" value="1"/>
0224	<ProtocolVersionMinor type="Integer" value="0"/>
0225	</ProtocolVersion>
0226	<BatchCount type="Integer" value="1"/>
0227	</RequestHeader>
0228	<BatchItem>
0229	<Operation type="Enumeration" value="GetAttributes"/>
0230	<RequestPayload>
0231	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>

0232	<AttributeName type="TextString" value="Name"/>
0233	<AttributeName type="TextString" value="Contact Information"/>
0234	</RequestPayload>
0235	</BatchItem>
0236	</RequestMessage>
0237	<ResponseMessage>
0238	<ResponseHeader>
0239	<ProtocolVersion>
0240	<ProtocolVersionMajor type="Integer" value="1"/>
0241	<ProtocolVersionMinor type="Integer" value="0"/>
0242	</ProtocolVersion>
0243	<TimeStamp type="DateTime" value="2009-11-12T11:10:28+00:00"/>
0244	<BatchCount type="Integer" value="1"/>
0245	</ResponseHeader>
0246	<BatchItem>
0247	<Operation type="Enumeration" value="GetAttributes"/>
0248	<ResultStatus type="Enumeration" value="Success"/>
0249	<ResponsePayload>
0250	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0251	<Attribute>
0252	<AttributeName type="TextString" value="Name"/>
0253	<AttributeValue>
0254	<NameValue type="TextString" value="Key1"/>
0255	<NameType type="Enumeration" value="UninterpretedTextString"/>
0256	</AttributeValue>
0257	</Attribute>
0258	<Attribute>
0259	<AttributeName type="TextString" value="Contact Information"/>
0260	<AttributeValue type="TextString" value="Foo"/>
0261	</Attribute>
0262	</ResponsePayload>
0263	</BatchItem>
0264	</ResponseMessage>
	# TIME 5
0265	<RequestMessage>
0266	<RequestHeader>
0267	<ProtocolVersion>
0268	<ProtocolVersionMajor type="Integer" value="1"/>
0269	<ProtocolVersionMinor type="Integer" value="0"/>
0270	</ProtocolVersion>
0271	<BatchCount type="Integer" value="2"/>
0272	</RequestHeader>
0273	<BatchItem>
0274	<Operation type="Enumeration" value="AddAttribute"/>
0275	<UniqueBatchItemID type="ByteString" value="7a92dda525eb158a"/>
0276	<RequestPayload>
0277	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0278	<Attribute>
0279	<AttributeName type="TextString" value="x-attribute1"/>
0280	<AttributeValue type="TextString" value="Value1"/>
0281	</Attribute>
0282	</RequestPayload>
0283	</BatchItem>

0284	<BatchItem>
0285	<Operation type="Enumeration" value="AddAttribute"/>
0286	<UniqueBatchItemID type="ByteString" value="7230f6e4d3bea249"/>
0287	<RequestPayload>
0288	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0289	<Attribute>
0290	<AttributeName type="TextString" value="x-attribute2"/>
0291	<AttributeValue type="TextString" value="Value2"/>
0292	</Attribute>
0293	</RequestPayload>
0294	</BatchItem>
0295	</RequestMessage>
0296	<ResponseMessage>
0297	<ResponseHeader>
0298	<ProtocolVersion>
0299	<ProtocolVersionMajor type="Integer" value="1"/>
0300	<ProtocolVersionMinor type="Integer" value="0"/>
0301	</ProtocolVersion>
0302	<TimeStamp type="DateTime" value="2009-11-12T11:10:29+00:00"/>
0303	<BatchCount type="Integer" value="2"/>
0304	</ResponseHeader>
0305	<BatchItem>
0306	<Operation type="Enumeration" value="AddAttribute"/>
0307	<UniqueBatchItemID type="ByteString" value="7a92dda525eb158a"/>
0308	<ResultStatus type="Enumeration" value="Success"/>
0309	<ResponsePayload>
0310	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0311	<Attribute>
0312	<AttributeName type="TextString" value="x-attribute1"/>
0313	<AttributeValue type="TextString" value="Value1"/>
0314	</Attribute>
0315	</ResponsePayload>
0316	</BatchItem>
0317	<BatchItem>
0318	<Operation type="Enumeration" value="AddAttribute"/>
0319	<UniqueBatchItemID type="ByteString" value="7230f6e4d3bea249"/>
0320	<ResultStatus type="Enumeration" value="Success"/>
0321	<ResponsePayload>
0322	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0323	<Attribute>
0324	<AttributeName type="TextString" value="x-attribute2"/>
0325	<AttributeValue type="TextString" value="Value2"/>
0326	</Attribute>
0327	</ResponsePayload>
0328	</BatchItem>
0329	</ResponseMessage>
	# TIME 6
0330	<RequestMessage>
0331	<RequestHeader>
0332	<ProtocolVersion>
0333	<ProtocolVersionMajor type="Integer" value="1"/>
0334	<ProtocolVersionMinor type="Integer" value="0"/>
0335	</ProtocolVersion>
0336	<BatchCount type="Integer" value="2"/>

```
0337 </RequestHeader>
0338 <BatchItem>
0339   <Operation type="Enumeration" value="ModifyAttribute"/>
0340   <UniqueBatchItemID type="ByteString" value="ba3ea60548ecb699"/>
0341   <RequestPayload>
0342     <UniqueIdentifier type="TextString"
0343     value="$UNIQUE_IDENTIFIER_1"/>
0344     <Attribute>
0345       <AttributeName type="TextString" value="x-attribute1"/>
0346       <AttributeValue type="TextString" value="ModifiedValue1"/>
0347     </Attribute>
0348   </RequestPayload>
0349 </BatchItem>
0350 <BatchItem>
0351   <Operation type="Enumeration" value="ModifyAttribute"/>
0352   <UniqueBatchItemID type="ByteString" value="321984e716274a3d"/>
0353   <RequestPayload>
0354     <UniqueIdentifier type="TextString"
0355     value="$UNIQUE_IDENTIFIER_1"/>
0356     <Attribute>
0357       <AttributeName type="TextString" value="x-attribute2"/>
0358       <AttributeValue type="TextString" value="ModifiedValue2"/>
0359     </Attribute>
0360   </RequestPayload>
0361 </BatchItem>
0362 </RequestMessage>
0363 <ResponseMessage>
0364   <ResponseHeader>
0365     <ProtocolVersion>
0366       <ProtocolVersionMajor type="Integer" value="1"/>
0367       <ProtocolVersionMinor type="Integer" value="0"/>
0368     </ProtocolVersion>
0369     <TimeStamp type="DateTime" value="2009-11-12T11:10:30+00:00"/>
0370     <BatchCount type="Integer" value="2"/>
0371   </ResponseHeader>
0372   <BatchItem>
0373     <Operation type="Enumeration" value="ModifyAttribute"/>
0374     <UniqueBatchItemID type="ByteString" value="ba3ea60548ecb699"/>
0375     <ResultStatus type="Enumeration" value="Success"/>
0376     <ResponsePayload>
0377       <UniqueIdentifier type="TextString"
0378       value="$UNIQUE_IDENTIFIER_1"/>
0379       <Attribute>
0380         <AttributeName type="TextString" value="x-attribute1"/>
0381         <AttributeValue type="TextString" value="ModifiedValue1"/>
0382       </Attribute>
0383     </ResponsePayload>
0384   </BatchItem>
0385   <BatchItem>
0386     <Operation type="Enumeration" value="ModifyAttribute"/>
0387     <UniqueBatchItemID type="ByteString" value="321984e716274a3d"/>
0388     <ResultStatus type="Enumeration" value="Success"/>
0389     <ResponsePayload>
0390       <UniqueIdentifier type="TextString"
0391       value="$UNIQUE_IDENTIFIER_1"/>
0392       <Attribute>
0393         <AttributeName type="TextString" value="x-attribute2"/>
```

0390	<AttributeValue type="TextString" value="ModifiedValue2"/>
0391	</Attribute>
0392	</ResponsePayload>
0393	</BatchItem>
0394	</ResponseMessage>
# TIME 7	
0395	<RequestMessage>
0396	<RequestHeader>
0397	<ProtocolVersion>
0398	<ProtocolVersionMajor type="Integer" value="1"/>
0399	<ProtocolVersionMinor type="Integer" value="0"/>
0400	</ProtocolVersion>
0401	<BatchCount type="Integer" value="2"/>
0402	</RequestHeader>
0403	<BatchItem>
0404	<Operation type="Enumeration" value="DeleteAttribute"/>
0405	<UniqueBatchItemID type="ByteString" value="d5c6df842daeecd8"/>
0406	<RequestPayload>
0407	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0408	<AttributeName type="TextString" value="x-attribute1"/>
0409	</RequestPayload>
0410	</BatchItem>
0411	<BatchItem>
0412	<Operation type="Enumeration" value="DeleteAttribute"/>
0413	<UniqueBatchItemID type="ByteString" value="572d4f0d433dab10"/>
0414	<RequestPayload>
0415	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0416	<AttributeName type="TextString" value="x-attribute2"/>
0417	</RequestPayload>
0418	</BatchItem>
0419	</RequestMessage>
0420	<ResponseMessage>
0421	<ResponseHeader>
0422	<ProtocolVersion>
0423	<ProtocolVersionMajor type="Integer" value="1"/>
0424	<ProtocolVersionMinor type="Integer" value="0"/>
0425	</ProtocolVersion>
0426	<TimeStamp type="DateTime" value="2009-11-12T11:10:30+00:00"/>
0427	<BatchCount type="Integer" value="2"/>
0428	</ResponseHeader>
0429	<BatchItem>
0430	<Operation type="Enumeration" value="DeleteAttribute"/>
0431	<UniqueBatchItemID type="ByteString" value="d5c6df842daeecd8"/>
0432	<ResultStatus type="Enumeration" value="Success"/>
0433	<ResponsePayload>
0434	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0435	<Attribute>
0436	<AttributeName type="TextString" value="x-attribute1"/>
0437	<AttributeValue type="TextString" value="ModifiedValue1"/>
0438	</Attribute>
0439	</ResponsePayload>
0440	</BatchItem>
0441	<BatchItem>
0442	<Operation type="Enumeration" value="DeleteAttribute"/>

0443	<UniqueBatchItemID type="ByteString" value="572d4f0d433dab10"/>
0444	<ResultStatus type="Enumeration" value="Success"/>
0445	<ResponsePayload>
0446	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0447	<Attribute>
0448	<AttributeName type="TextString" value="x-attribute2"/>
0449	<AttributeValue type="TextString" value="ModifiedValue2"/>
0450	</Attribute>
0451	</ResponsePayload>
0452	</BatchItem>
0453	</ResponseMessage>
	# TIME 8
0454	<RequestMessage>
0455	<RequestHeader>
0456	<ProtocolVersion>
0457	<ProtocolVersionMajor type="Integer" value="1"/>
0458	<ProtocolVersionMinor type="Integer" value="0"/>
0459	</ProtocolVersion>
0460	<BatchCount type="Integer" value="1"/>
0461	</RequestHeader>
0462	<BatchItem>
0463	<Operation type="Enumeration" value="Destroy"/>
0464	<RequestPayload>
0465	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0466	</RequestPayload>
0467	</BatchItem>
0468	</RequestMessage>
0469	<ResponseMessage>
0470	<ResponseHeader>
0471	<ProtocolVersion>
0472	<ProtocolVersionMajor type="Integer" value="1"/>
0473	<ProtocolVersionMinor type="Integer" value="0"/>
0474	</ProtocolVersion>
0475	<TimeStamp type="DateTime" value="2009-11-12T11:10:31+00:00"/>
0476	<BatchCount type="Integer" value="1"/>
0477	</ResponseHeader>
0478	<BatchItem>
0479	<Operation type="Enumeration" value="Destroy"/>
0480	<ResultStatus type="Enumeration" value="Success"/>
0481	<ResponsePayload>
0482	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0483	</ResponsePayload>
0484	</BatchItem>
0485	</ResponseMessage>
	# TIME 9
0486	<RequestMessage>
0487	<RequestHeader>
0488	<ProtocolVersion>
0489	<ProtocolVersionMajor type="Integer" value="1"/>
0490	<ProtocolVersionMinor type="Integer" value="0"/>
0491	</ProtocolVersion>
0492	<BatchCount type="Integer" value="1"/>
0493	</RequestHeader>

0494	<BatchItem>
0495	<Operation type="Enumeration" value="Get"/>
0496	<RequestPayload>
0497	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0498	</RequestPayload>
0499	</BatchItem>
0500	</RequestMessage>
0501	<ResponseMessage>
0502	<ResponseHeader>
0503	<ProtocolVersion>
0504	<ProtocolVersionMajor type="Integer" value="1"/>
0505	<ProtocolVersionMinor type="Integer" value="0"/>
0506	</ProtocolVersion>
0507	<TimeStamp type="DateTime" value="2009-11-12T11:10:31+00:00"/>
0508	<BatchCount type="Integer" value="1"/>
0509	</ResponseHeader>
0510	<BatchItem>
0511	<Operation type="Enumeration" value="Get"/>
0512	<ResultStatus type="Enumeration" value="OperationFailed"/>
0513	<ResultReason type="Enumeration" value="ItemNotFound"/>
0514	<ResultMessage type="TextString" value="Object does not exist"/>
0515	</BatchItem>
0516	</ResponseMessage>
# TIME 10	
0517	<RequestMessage>
0518	<RequestHeader>
0519	<ProtocolVersion>
0520	<ProtocolVersionMajor type="Integer" value="1"/>
0521	<ProtocolVersionMinor type="Integer" value="0"/>
0522	</ProtocolVersion>
0523	<BatchCount type="Integer" value="1"/>
0524	</RequestHeader>
0525	<BatchItem>
0526	<Operation type="Enumeration" value="Destroy"/>
0527	<RequestPayload>
0528	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0529	</RequestPayload>
0530	</BatchItem>
0531	</RequestMessage>
0532	<ResponseMessage>
0533	<ResponseHeader>
0534	<ProtocolVersion>
0535	<ProtocolVersionMajor type="Integer" value="1"/>
0536	<ProtocolVersionMinor type="Integer" value="0"/>
0537	</ProtocolVersion>
0538	<TimeStamp type="DateTime" value="2009-11-12T11:10:31+00:00"/>
0539	<BatchCount type="Integer" value="1"/>
0540	</ResponseHeader>
0541	<BatchItem>
0542	<Operation type="Enumeration" value="Destroy"/>
0543	<ResultStatus type="Enumeration" value="Success"/>
0544	<ResponsePayload>
0545	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0546	</ResponsePayload>
0547	</BatchItem>
0548	</ResponseMessage>
# TIME 11	
0549	<RequestMessage>
0550	<RequestHeader>
0551	<ProtocolVersion>
0552	<ProtocolVersionMajor type="Integer" value="1"/>
0553	<ProtocolVersionMinor type="Integer" value="0"/>
0554	</ProtocolVersion>
0555	<BatchCount type="Integer" value="1"/>
0556	</RequestHeader>
0557	<BatchItem>
0558	<Operation type="Enumeration" value="Get"/>
0559	<RequestPayload>
0560	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0561	</RequestPayload>
0562	</BatchItem>
0563	</RequestMessage>
0564	<ResponseMessage>
0565	<ResponseHeader>
0566	<ProtocolVersion>
0567	<ProtocolVersionMajor type="Integer" value="1"/>
0568	<ProtocolVersionMinor type="Integer" value="0"/>
0569	</ProtocolVersion>
0570	<TimeStamp type="DateTime" value="2009-11-12T11:10:31+00:00"/>
0571	<BatchCount type="Integer" value="1"/>
0572	</ResponseHeader>
0573	<BatchItem>
0574	<Operation type="Enumeration" value="Get"/>
0575	<ResultStatus type="Enumeration" value="OperationFailed"/>
0576	<ResultReason type="Enumeration" value="ItemNotFound"/>
0577	<ResultMessage type="TextString" value="No Cryptographic Object
	found with given Unique Identifier"/>
0578	</BatchItem>
0579	</ResponseMessage>

71

72 2.1.5 TC-315-10 - Register / Destroy Secret Data

73 In this test case the client issues a Register request containing a Secret Data object, whereby the
74 server registers the object and returns the Unique Identifier. To clean up, the client then
75 performs a Destroy operation to destroy the object.

# TIME 0	
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion> <BatchCount type="Integer" value="1"/>
0007	</RequestHeader> <BatchItem>
0008	<Operation type="Enumeration"
	value="Register"/> <RequestPayload>
0009	<ObjectType type="Enumeration" value="SecretData"/>

0010	<TemplateAttribute>
0011	<Attribute>
0012	<AttributeName type="TextString" value="Cryptographic Usage Mask"/> <AttributeValue type="Integer" value="Verify"/>
0013	</Attribute>
0014	</TemplateAttribute> <SecretData>
0015	<SecretDataType type="Enumeration" value="Password"/> <KeyBlock>
0016	<KeyFormatType type="Enumeration" value="Opaque"/> <KeyValue>
0017	<KeyMaterial type="ByteString" value="53656372657450617373776f7264"/>
0018	</KeyValue>
0019	</KeyBlock>
0020	</SecretData>
0021	</RequestPayload>
0022	</BatchItem>
0023	</RequestMessage>
0024	<ResponseMessage>
0025	<ResponseHeader>
0026	<ProtocolVersion>
0027	<ProtocolVersionMajor type="Integer" value="1"/>
0028	<ProtocolVersionMinor type="Integer" value="0"/>
0029	</ProtocolVersion>
0030	<TimeStamp type="DateTime" value="2010-02-15T10:41:21+00:00"/>
0031	<BatchCount type="Integer" value="1"/>
0032	</ResponseHeader>
0033	<BatchItem>
0034	<Operation type="Enumeration" value="Register"/>
0035	<ResultStatus type="Enumeration" value="Success"/>
0036	<ResponsePayload>
0037	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0038	</ResponsePayload>
0039	</BatchItem>
0040	</ResponseMessage>
	# TIME 1
0041	<RequestMessage>
0042	<RequestHeader>
0043	<ProtocolVersion>
0044	<ProtocolVersionMajor type="Integer" value="1"/>
0045	<ProtocolVersionMinor type="Integer" value="0"/>
0046	</ProtocolVersion>
0047	<BatchCount type="Integer" value="1"/>
0048	</RequestHeader>
0049	<BatchItem>
0050	<Operation type="Enumeration" value="Destroy"/>
0051	<RequestPayload>
0052	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0053	</RequestPayload>
0054	</BatchItem>
0055	</RequestMessage>
0056	<ResponseMessage>
0057	<ResponseHeader>
0058	<ProtocolVersion>


```
0059     <ProtocolVersionMajor type="Integer" value="1"/>
0060     <ProtocolVersionMinor type="Integer" value="0"/>
0061     </ProtocolVersion>
0062     <TimeStamp type="DateTime" value="2010-02-15T10:41:21+00:00"/>
0063     <BatchCount type="Integer" value="1"/>
0064 </ResponseHeader>
0065 <BatchItem>
0066     <Operation type="Enumeration" value="Destroy"/>
0067     <ResultStatus type="Enumeration" value="Success"/>
0068     <ResponsePayload>
0069         <UniqueIdentifier type="TextString"
value="$UNIQUE IDENTIFIER 0"/>
0070     </ResponsePayload>
0071 </BatchItem>
0072 </ResponseMessage>
```

76

77 2.1.6 TC-32-10 - Asynchronous Locate

78 This test case tests the asynchronous capabilities of KMIP using the Locate operation. A key is
79 created and then a Locate request is sent containing the Name of the created key and with the
80 message header Asynchronous Indicator-field set to True. If the server returns an asynchronous
81 response to the Locate, the client then polls the server until the operation is ready. If the server
82 responded asynchronously, a subsequent Locate operation that is also handled asynchronously
83 is then Canceled, before the key is finally destroyed.

84 This test case shows the use of two clients with the same assumptions as in the test case
85 described in Section . Since the client is unable to force the server to respond asynchronously, it
86 is possible for a server to respond synchronously to the requests issued at times 1 and 4, in
87 which case the expected response are the ones shown at times 2 and 5, respectively. In the case
88 of the server not responding asynchronously to the Locate requests, the client is permitted to
89 skip the requests illustrated at time 7 and 8.

```
0001 # TIME 0
0002 <RequestMessage>
0003     <RequestHeader>
0004         <ProtocolVersion>
0005             <ProtocolVersionMajor type="Integer" value="1"/>
0006             <ProtocolVersionMinor type="Integer" value="0"/>
0007         </ProtocolVersion>
0008         <BatchCount type="Integer" value="1"/>
0009     </RequestHeader>
0010     <BatchItem>
0011         <Operation type="Enumeration" value="Create"/>
0012         <RequestPayload>
0013             <ObjectType type="Enumeration" value="SymmetricKey"/>
0014             <TemplateAttribute>
0015                 <Attribute>
0016                     <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0017                     <AttributeValue type="Enumeration" value="AES"/>
0018                 </Attribute>
```

0019	<AttributeName type="TextString" value="Cryptographic
0020	Length"/>
0021	<AttributeValue type="Integer" value="128"/>
0022	</Attribute>
0023	<AttributeName type="TextString" value="Name"/>
0024	<AttributeValue>
0025	<NameValue type="TextString" value="Key1"/>
0026	<NameType type="Enumeration"
0027	value="UninterpretedTextString"/>
0028	</AttributeValue>
0029	</Attribute>
0030	<AttributeName type="TextString" value="Cryptographic
0031	Usage Mask"/>
0032	<AttributeValue type="Integer" value="Encrypt"/>
0033	</Attribute>
0034	<AttributeName type="TextString" value="Object Group"/>
0035	<AttributeValue type="TextString" value="Group1"/>
0036	</Attribute>
0037	</TemplateAttribute>
0038	</RequestPayload>
0039	</BatchItem>
0040	</RequestMessage>
0041	<ResponseMessage>
0042	<ResponseHeader>
0043	<ProtocolVersion>
0044	<ProtocolVersionMajor type="Integer" value="1"/>
0045	<ProtocolVersionMinor type="Integer" value="0"/>
0046	</ProtocolVersion>
0047	<TimeStamp type="DateTime" value="2009-11-12T11:10:32+00:00"/>
0048	<BatchCount type="Integer" value="1"/>
0049	</ResponseHeader>
0050	<BatchItem>
0051	<Operation type="Enumeration" value="Create"/>
0052	<ResultStatus type="Enumeration" value="Success"/>
0053	<ResponsePayload>
0054	<ObjectType type="Enumeration" value="SymmetricKey"/>
0055	<UniqueIdentifier type="TextString"
0056	value="\$UNIQUE_IDENTIFIER_0"/>
0057	</ResponsePayload>
0058	</BatchItem>
0059	</ResponseMessage>
0060	# TIME 1
0061	<RequestMessage>
0062	<RequestHeader>
0063	<ProtocolVersion>
0064	<ProtocolVersionMajor type="Integer" value="1"/>
0065	<ProtocolVersionMinor type="Integer" value="0"/>
0066	</ProtocolVersion>
0067	<AsynchronousIndicator type="Boolean" value="true"/>
0068	<BatchCount type="Integer" value="1"/>
0069	</RequestHeader>
0070	<BatchItem>
0071	<Operation type="Enumeration" value="Locate"/>
0072	<RequestPayload>

0071	<Attribute>
0072	<AttributeName type="TextString" value="Object Type"/>
0073	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0074	</Attribute>
0075	<Attribute>
0076	<AttributeName type="TextString" value="Name"/>
0077	<AttributeValue>
0078	<NameValue type="TextString" value="Key1"/>
0079	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0080	</AttributeValue>
0081	</Attribute>
0082	</RequestPayload>
0083	</BatchItem>
0084	</RequestMessage>
0085	<ResponseMessage>
0086	<ResponseHeader>
0087	<ProtocolVersion>
0088	<ProtocolVersionMajor type="Integer" value="1"/>
0089	<ProtocolVersionMinor type="Integer" value="0"/>
0090	</ProtocolVersion>
0091	<TimeStamp type="DateTime" value="2009-11-12T11:10:32+00:00"/>
0092	<BatchCount type="Integer" value="1"/>
0093	</ResponseHeader>
0094	<BatchItem>
0095	<Operation type="Enumeration" value="Locate"/>
0096	<ResultStatus type="Enumeration" value="OperationPending"/>
0097	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0098	</BatchItem>
0099	</ResponseMessage>
	# TIME 2
0100	<RequestMessage>
0101	<RequestHeader>
0102	<ProtocolVersion>
0103	<ProtocolVersionMajor type="Integer" value="1"/>
0104	<ProtocolVersionMinor type="Integer" value="0"/>
0105	</ProtocolVersion>
0106	<BatchCount type="Integer" value="1"/>
0107	</RequestHeader>
0108	<BatchItem>
0109	<Operation type="Enumeration" value="Poll"/>
0110	<RequestPayload>
0111	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0112	</RequestPayload>
0113	</BatchItem>
0114	</RequestMessage>
0115	<ResponseMessage>
0116	<ResponseHeader>
0117	<ProtocolVersion>
0118	<ProtocolVersionMajor type="Integer" value="1"/>
0119	<ProtocolVersionMinor type="Integer" value="0"/>
0120	</ProtocolVersion>
0121	<TimeStamp type="DateTime" value="2009-11-12T11:10:32+00:00"/>
0122	<BatchCount type="Integer" value="1"/>

0123	</ResponseHeader>
0124	<BatchItem>
0125	<Operation type="Enumeration" value="Locate"/>
0126	<ResultStatus type="Enumeration" value="Success"/>
0127	<ResponsePayload>
0128	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0129	</ResponsePayload>
0130	</BatchItem>
0131	</ResponseMessage>
# TIME 3	
0132	<RequestMessage>
0133	<RequestHeader>
0134	<ProtocolVersion>
0135	<ProtocolVersionMajor type="Integer" value="1"/>
0136	<ProtocolVersionMinor type="Integer" value="0"/>
0137	</ProtocolVersion>
0138	<BatchCount type="Integer" value="1"/>
0139	</RequestHeader>
0140	<BatchItem>
0141	<Operation type="Enumeration" value="Get"/>
0142	<RequestPayload>
0143	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0144	</RequestPayload>
0145	</BatchItem>
0146	</RequestMessage>
0147	<ResponseMessage>
0148	<ResponseHeader>
0149	<ProtocolVersion>
0150	<ProtocolVersionMajor type="Integer" value="1"/>
0151	<ProtocolVersionMinor type="Integer" value="0"/>
0152	</ProtocolVersion>
0153	<TimeStamp type="DateTime" value="2009-11-12T11:10:33+00:00"/>
0154	<BatchCount type="Integer" value="1"/>
0155	</ResponseHeader>
0156	<BatchItem>
0157	<Operation type="Enumeration" value="Get"/>
0158	<ResultStatus type="Enumeration" value="Success"/>
0159	<ResponsePayload>
0160	<ObjectType type="Enumeration" value="SymmetricKey"/>
0161	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0162	<SymmetricKey>
0163	<KeyBlock>
0164	<KeyFormatType type="Enumeration" value="Raw"/>
0165	<KeyValue>
0166	<KeyMaterial type="ByteString"
	value="bef01f82dfb4682a01c2a08413834aab"/>
0167	</KeyValue>
0168	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0169	<CryptographicLength type="Integer" value="128"/>
0170	</KeyBlock>
0171	</SymmetricKey>
0172	</ResponsePayload>
0173	</BatchItem>
0174	</ResponseMessage>

0175	# TIME 4
0176	<RequestMessage>
0177	<RequestHeader>
0178	<ProtocolVersion>
0179	<ProtocolVersionMajor type="Integer" value="1"/>
0180	<ProtocolVersionMinor type="Integer" value="0"/>
0181	</ProtocolVersion>
0182	<AsynchronousIndicator type="Boolean" value="true"/>
0183	<BatchCount type="Integer" value="1"/>
0184	</RequestHeader>
0185	<BatchItem>
0186	<Operation type="Enumeration" value="Locate"/>
0187	<RequestPayload>
0188	<Attribute>
0189	<AttributeName type="TextString" value="Object Type"/>
0190	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0191	</Attribute>
0192	<Attribute>
0193	<AttributeName type="TextString" value="Object Group"/>
0194	<AttributeValue type="TextString" value="Group1"/>
0195	</Attribute>
0196	</RequestPayload>
0197	</BatchItem>
0198	</RequestMessage>
0198	<ResponseMessage>
0199	<ResponseHeader>
0200	<ProtocolVersion>
0201	<ProtocolVersionMajor type="Integer" value="1"/>
0202	<ProtocolVersionMinor type="Integer" value="0"/>
0203	</ProtocolVersion>
0204	<TimeStamp type="DateTime" value="2009-11-12T11:10:33+00:00"/>
0205	<BatchCount type="Integer" value="1"/>
0206	</ResponseHeader>
0207	<BatchItem>
0208	<Operation type="Enumeration" value="Locate"/>
0209	<ResultStatus type="Enumeration" value="OperationPending"/>
0210	<AsynchronousCorrelationValue type="ByteString"
0211	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0212	</BatchItem>
0212	</ResponseMessage>
0213	# TIME 5
0214	<RequestMessage>
0215	<RequestHeader>
0216	<ProtocolVersion>
0217	<ProtocolVersionMajor type="Integer" value="1"/>
0218	<ProtocolVersionMinor type="Integer" value="0"/>
0219	</ProtocolVersion>
0220	<BatchCount type="Integer" value="1"/>
0221	</RequestHeader>
0222	<BatchItem>
0223	<Operation type="Enumeration" value="Poll"/>
0224	<RequestPayload>
0225	<AsynchronousCorrelationValue type="ByteString"
0226	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0227	</RequestPayload>
0227	</BatchItem>
0227	</RequestMessage>

0228	<ResponseMessage>
0229	<ResponseHeader>
0230	<ProtocolVersion>
0231	<ProtocolVersionMajor type="Integer" value="1"/>
0232	<ProtocolVersionMinor type="Integer" value="0"/>
0233	</ProtocolVersion>
0234	<TimeStamp type="DateTime" value="2009-11-12T11:10:33+00:00"/>
0235	<BatchCount type="Integer" value="1"/>
0236	</ResponseHeader>
0237	<BatchItem>
0238	<Operation type="Enumeration" value="Locate"/>
0239	<ResultStatus type="Enumeration" value="Success"/>
0240	<ResponsePayload>
0241	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0242	</ResponsePayload>
0243	</BatchItem>
0244	</ResponseMessage>
# TIME 6	
0245	<RequestMessage>
0246	<RequestHeader>
0247	<ProtocolVersion>
0248	<ProtocolVersionMajor type="Integer" value="1"/>
0249	<ProtocolVersionMinor type="Integer" value="0"/>
0250	</ProtocolVersion>
0251	<BatchCount type="Integer" value="1"/>
0252	</RequestHeader>
0253	<BatchItem>
0254	<Operation type="Enumeration" value="Get"/>
0255	<RequestPayload>
0256	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0257	</RequestPayload>
0258	</BatchItem>
0259	</RequestMessage>
0260	<ResponseMessage>
0261	<ResponseHeader>
0262	<ProtocolVersion>
0263	<ProtocolVersionMajor type="Integer" value="1"/>
0264	<ProtocolVersionMinor type="Integer" value="0"/>
0265	</ProtocolVersion>
0266	<TimeStamp type="DateTime" value="2009-11-12T11:10:33+00:00"/>
0267	<BatchCount type="Integer" value="1"/>
0268	</ResponseHeader>
0269	<BatchItem>
0270	<Operation type="Enumeration" value="Get"/>
0271	<ResultStatus type="Enumeration" value="Success"/>
0272	<ResponsePayload>
0273	<ObjectType type="Enumeration" value="SymmetricKey"/>
0274	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0275	<SymmetricKey>
0276	<KeyBlock>
0277	<KeyFormatType type="Enumeration" value="Raw"/>
0278	<KeyValue>
0279	<KeyMaterial type="ByteString"
	value="bef01f82dfb4682a01c2a08413834aab"/>

0280	</KeyValue>
0281	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0282	<CryptographicLength type="Integer" value="128"/>
0283	</KeyBlock>
0284	</SymmetricKey>
0285	</ResponsePayload>
0286	</BatchItem>
0287	</ResponseMessage>
# TIME 7	
0288	<RequestMessage>
0289	<RequestHeader>
0290	<ProtocolVersion>
0291	<ProtocolVersionMajor type="Integer" value="1"/>
0292	<ProtocolVersionMinor type="Integer" value="0"/>
0293	</ProtocolVersion>
0294	<AsynchronousIndicator type="Boolean" value="true"/>
0295	<BatchCount type="Integer" value="1"/>
0296	</RequestHeader>
0297	<BatchItem>
0298	<Operation type="Enumeration" value="Locate"/>
0299	<RequestPayload>
0300	<Attribute>
0301	<AttributeName type="TextString" value="Object Type"/>
0302	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0303	</Attribute>
0304	<Attribute>
0305	<AttributeName type="TextString" value="Name"/>
0306	<AttributeValue>
0307	<NameValue type="TextString" value="Key1"/>
0308	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0309	</AttributeValue>
0310	</Attribute>
0311	</RequestPayload>
0312	</BatchItem>
0313	</RequestMessage>
0314	<ResponseMessage>
0315	<ResponseHeader>
0316	<ProtocolVersion>
0317	<ProtocolVersionMajor type="Integer" value="1"/>
0318	<ProtocolVersionMinor type="Integer" value="0"/>
0319	</ProtocolVersion>
0320	<TimeStamp type="DateTime" value="2009-11-12T11:10:33+00:00"/>
0321	<BatchCount type="Integer" value="1"/>
0322	</ResponseHeader>
0323	<BatchItem>
0324	<Operation type="Enumeration" value="Locate"/>
0325	<ResultStatus type="Enumeration" value="OperationPending"/>
0326	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0327	</BatchItem>
0328	</ResponseMessage>
# TIME 8	
0329	<RequestMessage>
0330	<RequestHeader>
0331	<ProtocolVersion>

0332	<ProtocolVersionMajor type="Integer" value="1"/>
0333	<ProtocolVersionMinor type="Integer" value="0"/>
0334	</ProtocolVersion>
0335	<BatchCount type="Integer" value="1"/>
0336	</RequestHeader>
0337	<BatchItem>
0338	<Operation type="Enumeration" value="Cancel"/>
0339	<RequestPayload>
0340	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0341	</RequestPayload>
0342	</BatchItem>
0343	</RequestMessage>
0344	<ResponseMessage>
0345	<ResponseHeader>
0346	<ProtocolVersion>
0347	<ProtocolVersionMajor type="Integer" value="1"/>
0348	<ProtocolVersionMinor type="Integer" value="0"/>
0349	</ProtocolVersion>
0350	<TimeStamp type="DateTime" value="2009-11-12T11:10:33+00:00"/>
0351	<BatchCount type="Integer" value="1"/>
0352	</ResponseHeader>
0353	<BatchItem>
0354	<Operation type="Enumeration" value="Cancel"/>
0355	<ResultStatus type="Enumeration" value="Success"/>
0356	<ResponsePayload>
0357	<AsynchronousCorrelationValue type="ByteString"
	value="4d6bbfc35fe57fba"/>
0358	<CancellationResult type="Enumeration" value="Canceled"/>
0359	</ResponsePayload>
0360	</BatchItem>
0361	</ResponseMessage>
	# TIME 9
0362	<RequestMessage>
0363	<RequestHeader>
0364	<ProtocolVersion>
0365	<ProtocolVersionMajor type="Integer" value="1"/>
0366	<ProtocolVersionMinor type="Integer" value="0"/>
0367	</ProtocolVersion>
0368	<BatchCount type="Integer" value="1"/>
0369	</RequestHeader>
0370	<BatchItem>
0371	<Operation type="Enumeration" value="Destroy"/>
0372	<RequestPayload>
0373	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0374	</RequestPayload>
0375	</BatchItem>
0376	</RequestMessage>
0377	<ResponseMessage>
0378	<ResponseHeader>
0379	<ProtocolVersion>
0380	<ProtocolVersionMajor type="Integer" value="1"/>
0381	<ProtocolVersionMinor type="Integer" value="0"/>
0382	</ProtocolVersion>
0383	<TimeStamp type="DateTime" value="2009-11-12T11:10:34+00:00"/>


```
0384     <BatchCount type="Integer" value="1"/>
0385   </ResponseHeader>
0386   <BatchItem>
0387     <Operation type="Enumeration" value="Destroy"/>
0388     <ResultStatus type="Enumeration" value="Success"/>
0389     <ResponsePayload>
0390       <UniqueIdentifier type="TextString"
0391       value="$UNIQUE_IDENTIFIER_0"/>
0392     </ResponsePayload>
0393   </BatchItem>
0394 </ResponseMessage>
```

90

91 2.1.7 TC-41-10 - Revoke Scenario

92 This test case tests the revocation aspect of the key life cycle support in KMIP. A key is created
93 and a Get Attribute for the State-attribute reveals that the key is in Pre-active state. The
94 Activation Date is then set, which changes the state to Active. The key is then revoked with a
95 revocation reason of Compromised and the state subsequently changed to Compromised, but
96 this does not stop a client from being able to add, modify and delete attributes or even get the
97 key (since we assume here that the out-of-band registration has been used to make the server
98 aware of the fact that the client is capable of interpreting the attributes of the key and
99 determining what it is allowed to do with the key). To clean up, the created key is finally
100 destroyed.

```
0001 # TIME 0
0002 <RequestMessage>
0003   <RequestHeader>
0004     <ProtocolVersion>
0005       <ProtocolVersionMajor type="Integer" value="1"/>
0006       <ProtocolVersionMinor type="Integer" value="0"/>
0007     </ProtocolVersion>
0008     <BatchCount type="Integer" value="1"/>
0009   </RequestHeader>
0010   <BatchItem>
0011     <Operation type="Enumeration" value="Create"/>
0012     <RequestPayload>
0013       <ObjectType type="Enumeration" value="SymmetricKey"/>
0014       <TemplateAttribute>
0015         <Attribute>
0016           <AttributeName type="TextString" value="Cryptographic
0017           Algorithm"/>
0018           <AttributeValue type="Enumeration" value="AES"/>
0019         </Attribute>
0020         <Attribute>
0021           <AttributeName type="TextString" value="Cryptographic
0022           Length"/>
0023           <AttributeValue type="Integer" value="128"/>
0024         </Attribute>
0025         <Attribute>
0026           <AttributeName type="TextString" value="Name"/>
0027           <AttributeValue>
0028             <NameValue type="TextString" value="Key1"/>
0029             <NameType type="Enumeration"
```

0027	value="UninterpretedTextString"/>
0028	</AttributeValue>
0029	</Attribute>
0030	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0031	<AttributeValue type="Integer" value="Encrypt"/>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="0"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2009-11-12T11:10:35+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString"
0052	value="\$UNIQUE_IDENTIFIER_0"/>
0053	</ResponsePayload>
0054	</BatchItem>
0055	</ResponseMessage>
0056	# TIME 1
0057	<RequestMessage>
0058	<RequestHeader>
0059	<ProtocolVersion>
0060	<ProtocolVersionMajor type="Integer" value="1"/>
0061	<ProtocolVersionMinor type="Integer" value="0"/>
0062	</ProtocolVersion>
0063	<BatchCount type="Integer" value="1"/>
0064	</RequestHeader>
0065	<BatchItem>
0066	<Operation type="Enumeration" value="GetAttributes"/>
0067	<RequestPayload>
0068	<UniqueIdentifier type="TextString"
0069	value="\$UNIQUE_IDENTIFIER_0"/>
0070	<AttributeName type="TextString" value="State"/>
0071	</RequestPayload>
0072	</BatchItem>
0073	</RequestMessage>
0074	<ResponseMessage>
0075	<ResponseHeader>
0076	<ProtocolVersion>
0077	<ProtocolVersionMajor type="Integer" value="1"/>
	<ProtocolVersionMinor type="Integer" value="0"/>
	</ProtocolVersion>
	<TimeStamp type="DateTime" value="2009-11-12T11:10:35+00:00"/>

0078	<BatchCount type="Integer" value="1"/>
0079	</ResponseHeader>
0080	<BatchItem>
0081	<Operation type="Enumeration" value="GetAttributes"/>
0082	<ResultStatus type="Enumeration" value="Success"/>
0083	<ResponsePayload>
0084	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0085	<Attribute>
0086	<AttributeName type="TextString" value="State"/>
0087	<AttributeValue type="Enumeration" value="PreActive"/>
0088	</Attribute>
0089	</ResponsePayload>
0090	</BatchItem>
0091	</ResponseMessage>
	# TIME 2
0092	<RequestMessage>
0093	<RequestHeader>
0094	<ProtocolVersion>
0095	<ProtocolVersionMajor type="Integer" value="1"/>
0096	<ProtocolVersionMinor type="Integer" value="0"/>
0097	</ProtocolVersion>
0098	<BatchCount type="Integer" value="1"/>
0099	</RequestHeader>
0100	<BatchItem>
0101	<Operation type="Enumeration" value="Activate"/>
0102	<RequestPayload>
0103	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0104	</RequestPayload>
0105	</BatchItem>
0106	</RequestMessage>
0107	<ResponseMessage>
0108	<ResponseHeader>
0109	<ProtocolVersion>
0110	<ProtocolVersionMajor type="Integer" value="1"/>
0111	<ProtocolVersionMinor type="Integer" value="0"/>
0112	</ProtocolVersion>
0113	<TimeStamp type="DateTime" value="2009-11-12T11:10:35+00:00"/>
0114	<BatchCount type="Integer" value="1"/>
0115	</ResponseHeader>
0116	<BatchItem>
0117	<Operation type="Enumeration" value="Activate"/>
0118	<ResultStatus type="Enumeration" value="Success"/>
0119	<ResponsePayload>
0120	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0121	</ResponsePayload>
0122	</BatchItem>
0123	</ResponseMessage>
	# TIME 3
0124	<RequestMessage>
0125	<RequestHeader>
0126	<ProtocolVersion>
0127	<ProtocolVersionMajor type="Integer" value="1"/>
0128	<ProtocolVersionMinor type="Integer" value="0"/>

0129	</ProtocolVersion>
0130	<BatchCount type="Integer" value="1"/>
0131	</RequestHeader>
0132	<BatchItem>
0133	<Operation type="Enumeration" value="GetAttributes"/>
0134	<RequestPayload>
0135	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0136	<AttributeName type="TextString" value="State"/>
0137	</RequestPayload>
0138	</BatchItem>
0139	</RequestMessage>
0140	<ResponseMessage>
0141	<ResponseHeader>
0142	<ProtocolVersion>
0143	<ProtocolVersionMajor type="Integer" value="1"/>
0144	<ProtocolVersionMinor type="Integer" value="0"/>
0145	</ProtocolVersion>
0146	<TimeStamp type="DateTime" value="2009-11-12T11:10:35+00:00"/>
0147	<BatchCount type="Integer" value="1"/>
0148	</ResponseHeader>
0149	<BatchItem>
0150	<Operation type="Enumeration" value="GetAttributes"/>
0151	<ResultStatus type="Enumeration" value="Success"/>
0152	<ResponsePayload>
0153	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0154	<Attribute>
0155	<AttributeName type="TextString" value="State"/>
0156	<AttributeValue type="Enumeration" value="Active"/>
0157	</Attribute>
0158	</ResponsePayload>
0159	</BatchItem>
0160	</ResponseMessage>
	# TIME 4
0161	<RequestMessage>
0162	<RequestHeader>
0163	<ProtocolVersion>
0164	<ProtocolVersionMajor type="Integer" value="1"/>
0165	<ProtocolVersionMinor type="Integer" value="0"/>
0166	</ProtocolVersion>
0167	<BatchCount type="Integer" value="1"/>
0168	</RequestHeader>
0169	<BatchItem>
0170	<Operation type="Enumeration" value="Locate"/>
0171	<RequestPayload>
0172	<Attribute>
0173	<AttributeName type="TextString" value="Object Type"/>
0174	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0175	</Attribute>
0176	<Attribute>
0177	<AttributeName type="TextString" value="Name"/>
0178	<AttributeValue>
0179	<NameValue type="TextString" value="Key1"/>
0180	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0181	</AttributeValue>

0182	</Attribute>
0183	</RequestPayload>
0184	</BatchItem>
0185	</RequestMessage>
0186	<ResponseMessage>
0187	<ResponseHeader>
0188	<ProtocolVersion>
0189	<ProtocolVersionMajor type="Integer" value="1"/>
0190	<ProtocolVersionMinor type="Integer" value="0"/>
0191	</ProtocolVersion>
0192	<TimeStamp type="DateTime" value="2009-11-12T11:10:35+00:00"/>
0193	<BatchCount type="Integer" value="1"/>
0194	</ResponseHeader>
0195	<BatchItem>
0196	<Operation type="Enumeration" value="Locate"/>
0197	<ResultStatus type="Enumeration" value="Success"/>
0198	<ResponsePayload>
0199	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0200	</ResponsePayload>
0201	</BatchItem>
0202	</ResponseMessage>
0203	# TIME 5
0203	<RequestMessage>
0204	<RequestHeader>
0205	<ProtocolVersion>
0206	<ProtocolVersionMajor type="Integer" value="1"/>
0207	<ProtocolVersionMinor type="Integer" value="0"/>
0208	</ProtocolVersion>
0209	<BatchCount type="Integer" value="1"/>
0210	</RequestHeader>
0211	<BatchItem>
0212	<Operation type="Enumeration" value="Get"/>
0213	<RequestPayload>
0214	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0215	</RequestPayload>
0216	</BatchItem>
0217	</RequestMessage>
0218	<ResponseMessage>
0219	<ResponseHeader>
0220	<ProtocolVersion>
0221	<ProtocolVersionMajor type="Integer" value="1"/>
0222	<ProtocolVersionMinor type="Integer" value="0"/>
0223	</ProtocolVersion>
0224	<TimeStamp type="DateTime" value="2009-11-12T11:10:35+00:00"/>
0225	<BatchCount type="Integer" value="1"/>
0226	</ResponseHeader>
0227	<BatchItem>
0228	<Operation type="Enumeration" value="Get"/>
0229	<ResultStatus type="Enumeration" value="Success"/>
0230	<ResponsePayload>
0231	<ObjectType type="Enumeration" value="SymmetricKey"/>
0232	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0233	<SymmetricKey>

0234	<KeyBlock>
0235	<KeyFormatType type="Enumeration" value="Raw"/>
0236	<KeyValue>
0237	<KeyMaterial type="ByteString"
	value="ef7833ab15f5a1ee5874bc0d9bbc4be7"/>
0238	</KeyValue>
0239	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0240	<CryptographicLength type="Integer" value="128"/>
0241	</KeyBlock>
0242	</SymmetricKey>
0243	</ResponsePayload>
0244	</BatchItem>
0245	</ResponseMessage>
	# TIME 6
0246	<RequestMessage>
0247	<RequestHeader>
0248	<ProtocolVersion>
0249	<ProtocolVersionMajor type="Integer" value="1"/>
0250	<ProtocolVersionMinor type="Integer" value="0"/>
0251	</ProtocolVersion>
0252	<BatchCount type="Integer" value="1"/>
0253	</RequestHeader>
0254	<BatchItem>
0255	<Operation type="Enumeration" value="Revoke"/>
0256	<RequestPayload>
0257	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0258	<RevocationReason>
0259	<RevocationReasonCode type="Enumeration"
	value="KeyCompromise"/>
0260	</RevocationReason>
0261	<CompromiseOccurrenceDate type="DateTime" value="1970-01-
	01T00:00:00+00:00"/>
0262	</RequestPayload>
0263	</BatchItem>
0264	</RequestMessage>
0265	<ResponseMessage>
0266	<ResponseHeader>
0267	<ProtocolVersion>
0268	<ProtocolVersionMajor type="Integer" value="1"/>
0269	<ProtocolVersionMinor type="Integer" value="0"/>
0270	</ProtocolVersion>
0271	<TimeStamp type="DateTime" value="2009-11-12T11:10:35+00:00"/>
0272	<BatchCount type="Integer" value="1"/>
0273	</ResponseHeader>
0274	<BatchItem>
0275	<Operation type="Enumeration" value="Revoke"/>
0276	<ResultStatus type="Enumeration" value="Success"/>
0277	<ResponsePayload>
0278	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0279	</ResponsePayload>
0280	</BatchItem>
0281	</ResponseMessage>
	# TIME 7
0282	<RequestMessage>

0283	<RequestHeader>
0284	<ProtocolVersion>
0285	<ProtocolVersionMajor type="Integer" value="1"/>
0286	<ProtocolVersionMinor type="Integer" value="0"/>
0287	</ProtocolVersion>
0288	<BatchCount type="Integer" value="1"/>
0289	</RequestHeader>
0290	<BatchItem>
0291	<Operation type="Enumeration" value="GetAttributes"/>
0292	<RequestPayload>
0293	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0294	<AttributeName type="TextString" value="State"/>
0295	</RequestPayload>
0296	</BatchItem>
0297	</RequestMessage>
0298	<ResponseMessage>
0299	<ResponseHeader>
0300	<ProtocolVersion>
0301	<ProtocolVersionMajor type="Integer" value="1"/>
0302	<ProtocolVersionMinor type="Integer" value="0"/>
0303	</ProtocolVersion>
0304	<TimeStamp type="DateTime" value="2009-11-12T11:10:36+00:00"/>
0305	<BatchCount type="Integer" value="1"/>
0306	</ResponseHeader>
0307	<BatchItem>
0308	<Operation type="Enumeration" value="GetAttributes"/>
0309	<ResultStatus type="Enumeration" value="Success"/>
0310	<ResponsePayload>
0311	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0312	<Attribute>
0313	<AttributeName type="TextString" value="State"/>
0314	<AttributeValue type="Enumeration" value="Compromised"/>
0315	</Attribute>
0316	</ResponsePayload>
0317	</BatchItem>
0318	</ResponseMessage>
	# TIME 8
0319	<RequestMessage>
0320	<RequestHeader>
0321	<ProtocolVersion>
0322	<ProtocolVersionMajor type="Integer" value="1"/>
0323	<ProtocolVersionMinor type="Integer" value="0"/>
0324	</ProtocolVersion>
0325	<BatchCount type="Integer" value="1"/>
0326	</RequestHeader>
0327	<BatchItem>
0328	<Operation type="Enumeration" value="GetAttributeList"/>
0329	<RequestPayload>
0330	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0331	</RequestPayload>
0332	</BatchItem>
0333	</RequestMessage>
0334	<ResponseMessage>

0335	<ResponseHeader>
0336	<ProtocolVersion>
0337	<ProtocolVersionMajor type="Integer" value="1"/>
0338	<ProtocolVersionMinor type="Integer" value="0"/>
0339	</ProtocolVersion>
0340	<TimeStamp type="DateTime" value="2009-11-12T11:10:36+00:00"/>
0341	<BatchCount type="Integer" value="1"/>
0342	</ResponseHeader>
0343	<BatchItem>
0344	<Operation type="Enumeration" value="GetAttributeList"/>
0345	<ResultStatus type="Enumeration" value="Success"/>
0346	<ResponsePayload>
0347	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0348	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0349	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0350	<AttributeName type="TextString" value="State"/>
0351	<AttributeName type="TextString" value="Compromise Occurrence
	Date"/>
0352	<AttributeName type="TextString" value="Compromise Date"/>
0353	<AttributeName type="TextString" value="Digest"/>
0354	<AttributeName type="TextString" value="Initial Date"/>
0355	<AttributeName type="TextString" value="Activation Date"/>
0356	<AttributeName type="TextString" value="Revocation Reason"/>
0357	<AttributeName type="TextString" value="Unique Identifier"/>
0358	<AttributeName type="TextString" value="Name"/>
0359	<AttributeName type="TextString" value="Lease Time"/>
0360	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0361	<AttributeName type="TextString" value="Object Type"/>
0362	<AttributeName type="TextString" value="Last Change Date"/>
0363	</ResponsePayload>
0364	</BatchItem>
0365	</ResponseMessage>
	# TIME 9
0366	<RequestMessage>
0367	<RequestHeader>
0368	<ProtocolVersion>
0369	<ProtocolVersionMajor type="Integer" value="1"/>
0370	<ProtocolVersionMinor type="Integer" value="0"/>
0371	</ProtocolVersion>
0372	<BatchCount type="Integer" value="1"/>
0373	</RequestHeader>
0374	<BatchItem>
0375	<Operation type="Enumeration" value="GetAttributes"/>
0376	<RequestPayload>
0377	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0378	<AttributeName type="TextString" value="State"/>
0379	</RequestPayload>
0380	</BatchItem>
0381	</RequestMessage>
0382	<ResponseMessage>
0383	<ResponseHeader>
0384	<ProtocolVersion>

0385	<ProtocolVersionMajor type="Integer" value="1"/>
0386	<ProtocolVersionMinor type="Integer" value="0"/>
0387	</ProtocolVersion>
0388	<TimeStamp type="DateTime" value="2009-11-12T11:10:36+00:00"/>
0389	<BatchCount type="Integer" value="1"/>
0390	</ResponseHeader>
0391	<BatchItem>
0392	<Operation type="Enumeration" value="GetAttributes"/>
0393	<ResultStatus type="Enumeration" value="Success"/>
0394	<ResponsePayload>
0395	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER 0"/>
0396	<Attribute>
0397	<AttributeName type="TextString" value="State"/>
0398	<AttributeValue type="Enumeration" value="Compromised"/>
0399	</Attribute>
0400	</ResponsePayload>
0401	</BatchItem>
0402	</ResponseMessage>
	# TIME 10
0403	<RequestMessage>
0404	<RequestHeader>
0405	<ProtocolVersion>
0406	<ProtocolVersionMajor type="Integer" value="1"/>
0407	<ProtocolVersionMinor type="Integer" value="0"/>
0408	</ProtocolVersion>
0409	<BatchCount type="Integer" value="2"/>
0410	</RequestHeader>
0411	<BatchItem>
0412	<Operation type="Enumeration" value="AddAttribute"/>
0413	<UniqueBatchItemID type="ByteString" value="9d407ffb45c95672"/>
0414	<RequestPayload>
0415	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0416	<Attribute>
0417	<AttributeName type="TextString" value="x-attribute1"/>
0418	<AttributeValue type="TextString" value="Value1"/>
0419	</Attribute>
0420	</RequestPayload>
0421	</BatchItem>
0422	<BatchItem>
0423	<Operation type="Enumeration" value="AddAttribute"/>
0424	<UniqueBatchItemID type="ByteString" value="d62107c3158409d8"/>
0425	<RequestPayload>
0426	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0427	<Attribute>
0428	<AttributeName type="TextString" value="x-attribute2"/>
0429	<AttributeValue type="TextString" value="Value2"/>
0430	</Attribute>
0431	</RequestPayload>
0432	</BatchItem>
0433	</RequestMessage>
0434	<ResponseMessage>
0435	<ResponseHeader>
0436	<ProtocolVersion>
0437	<ProtocolVersionMajor type="Integer" value="1"/>

0438	<ProtocolVersionMinor type="Integer" value="0"/>
0439	</ProtocolVersion>
0440	<TimeStamp type="DateTime" value="2009-11-12T11:10:36+00:00"/>
0441	<BatchCount type="Integer" value="2"/>
0442	</ResponseHeader>
0443	<BatchItem>
0444	<Operation type="Enumeration" value="AddAttribute"/>
0445	<UniqueBatchItemID type="ByteString" value="9d407ffb45c95672"/>
0446	<ResultStatus type="Enumeration" value="Success"/>
0447	<ResponsePayload>
0448	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0449	<Attribute>
0450	<AttributeName type="TextString" value="x-attribute1"/>
0451	<AttributeValue type="TextString" value="Value1"/>
0452	</Attribute>
0453	</ResponsePayload>
0454	</BatchItem>
0455	<BatchItem>
0456	<Operation type="Enumeration" value="AddAttribute"/>
0457	<UniqueBatchItemID type="ByteString" value="d62107c3158409d8"/>
0458	<ResultStatus type="Enumeration" value="Success"/>
0459	<ResponsePayload>
0460	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0461	<Attribute>
0462	<AttributeName type="TextString" value="x-attribute2"/>
0463	<AttributeValue type="TextString" value="Value2"/>
0464	</Attribute>
0465	</ResponsePayload>
0466	</BatchItem>
0467	</ResponseMessage>
	# TIME 11
0468	<RequestMessage>
0469	<RequestHeader>
0470	<ProtocolVersion>
0471	<ProtocolVersionMajor type="Integer" value="1"/>
0472	<ProtocolVersionMinor type="Integer" value="0"/>
0473	</ProtocolVersion>
0474	<BatchCount type="Integer" value="2"/>
0475	</RequestHeader>
0476	<BatchItem>
0477	<Operation type="Enumeration" value="ModifyAttribute"/>
0478	<UniqueBatchItemID type="ByteString" value="47fb42cceca3f6ec"/>
0479	<RequestPayload>
0480	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0481	<Attribute>
0482	<AttributeName type="TextString" value="x-attribute1"/>
0483	<AttributeValue type="TextString" value="ModifiedValue1"/>
0484	</Attribute>
0485	</RequestPayload>
0486	</BatchItem>
0487	<BatchItem>
0488	<Operation type="Enumeration" value="ModifyAttribute"/>
0489	<UniqueBatchItemID type="ByteString" value="08019a230a05e9e1"/>
0490	<RequestPayload>

0491	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0492	<Attribute>
0493	<AttributeName type="TextString" value="x-attribute2"/>
0494	<AttributeValue type="TextString" value="ModifiedValue2"/>
0495	</Attribute>
0496	</RequestPayload>
0497	</BatchItem>
0498	</RequestMessage>
0499	<ResponseMessage>
0500	<ResponseHeader>
0501	<ProtocolVersion>
0502	<ProtocolVersionMajor type="Integer" value="1"/>
0503	<ProtocolVersionMinor type="Integer" value="0"/>
0504	</ProtocolVersion>
0505	<TimeStamp type="DateTime" value="2009-11-12T11:10:37+00:00"/>
0506	<BatchCount type="Integer" value="2"/>
0507	</ResponseHeader>
0508	<BatchItem>
0509	<Operation type="Enumeration" value="ModifyAttribute"/>
0510	<UniqueBatchItemID type="ByteString" value="47fb42cceca3f6ec"/>
0511	<ResultStatus type="Enumeration" value="Success"/>
0512	<ResponsePayload>
0513	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0514	<Attribute>
0515	<AttributeName type="TextString" value="x-attribute1"/>
0516	<AttributeValue type="TextString" value="ModifiedValue1"/>
0517	</Attribute>
0518	</ResponsePayload>
0519	</BatchItem>
0520	<BatchItem>
0521	<Operation type="Enumeration" value="ModifyAttribute"/>
0522	<UniqueBatchItemID type="ByteString" value="08019a230a05e9e1"/>
0523	<ResultStatus type="Enumeration" value="Success"/>
0524	<ResponsePayload>
0525	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0526	<Attribute>
0527	<AttributeName type="TextString" value="x-attribute2"/>
0528	<AttributeValue type="TextString" value="ModifiedValue2"/>
0529	</Attribute>
0530	</ResponsePayload>
0531	</BatchItem>
0532	</ResponseMessage>
	# TIME 12
0533	<RequestMessage>
0534	<RequestHeader>
0535	<ProtocolVersion>
0536	<ProtocolVersionMajor type="Integer" value="1"/>
0537	<ProtocolVersionMinor type="Integer" value="0"/>
0538	</ProtocolVersion>
0539	<BatchCount type="Integer" value="2"/>
0540	</RequestHeader>
0541	<BatchItem>
0542	<Operation type="Enumeration" value="DeleteAttribute"/>
0543	<UniqueBatchItemID type="ByteString" value="3e2c080fa8806057"/>

0544	<RequestPayload>
0545	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0546	<AttributeName type="TextString" value="x-attribute1"/>
0547	</RequestPayload>
0548	</BatchItem>
0549	<BatchItem>
0550	<Operation type="Enumeration" value="DeleteAttribute"/>
0551	<UniqueBatchItemID type="ByteString" value="9d55988d43d23b82"/>
0552	<RequestPayload>
0553	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0554	<AttributeName type="TextString" value="x-attribute2"/>
0555	</RequestPayload>
0556	</BatchItem>
0557	</RequestMessage>
0558	<ResponseMessage>
0559	<ResponseHeader>
0560	<ProtocolVersion>
0561	<ProtocolVersionMajor type="Integer" value="1"/>
0562	<ProtocolVersionMinor type="Integer" value="0"/>
0563	</ProtocolVersion>
0564	<TimeStamp type="DateTime" value="2009-11-12T11:10:37+00:00"/>
0565	<BatchCount type="Integer" value="2"/>
0566	</ResponseHeader>
0567	<BatchItem>
0568	<Operation type="Enumeration" value="DeleteAttribute"/>
0569	<UniqueBatchItemID type="ByteString" value="3e2c080fa8806057"/>
0570	<ResultStatus type="Enumeration" value="Success"/>
0571	<ResponsePayload>
0572	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0573	<Attribute>
0574	<AttributeName type="TextString" value="x-attribute1"/>
0575	<AttributeValue type="TextString" value="ModifiedValue1"/>
0576	</Attribute>
0577	</ResponsePayload>
0578	</BatchItem>
0579	<BatchItem>
0580	<Operation type="Enumeration" value="DeleteAttribute"/>
0581	<UniqueBatchItemID type="ByteString" value="9d55988d43d23b82"/>
0582	<ResultStatus type="Enumeration" value="Success"/>
0583	<ResponsePayload>
0584	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0585	<Attribute>
0586	<AttributeName type="TextString" value="x-attribute2"/>
0587	<AttributeValue type="TextString" value="ModifiedValue2"/>
0588	</Attribute>
0589	</ResponsePayload>
0590	</BatchItem>
0591	</ResponseMessage>
	# TIME 13
0592	<RequestMessage>
0593	<RequestHeader>
0594	<ProtocolVersion>
0595	<ProtocolVersionMajor type="Integer" value="1"/>

0596	<ProtocolVersionMinor type="Integer" value="0"/>
0597	</ProtocolVersion>
0598	<BatchCount type="Integer" value="1"/>
0599	</RequestHeader>
0600	<BatchItem>
0601	<Operation type="Enumeration" value="Get"/>
0602	<RequestPayload>
0603	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0604	</RequestPayload>
0605	</BatchItem>
0606	</RequestMessage>
0607	<ResponseMessage>
0608	<ResponseHeader>
0609	<ProtocolVersion>
0610	<ProtocolVersionMajor type="Integer" value="1"/>
0611	<ProtocolVersionMinor type="Integer" value="0"/>
0612	</ProtocolVersion>
0613	<TimeStamp type="DateTime" value="2009-11-12T11:10:37+00:00"/>
0614	<BatchCount type="Integer" value="1"/>
0615	</ResponseHeader>
0616	<BatchItem>
0617	<Operation type="Enumeration" value="Get"/>
0618	<ResultStatus type="Enumeration" value="Success"/>
0619	<ResponsePayload>
0620	<ObjectType type="Enumeration" value="SymmetricKey"/>
0621	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0622	<SymmetricKey>
0623	<KeyBlock>
0624	<KeyFormatType type="Enumeration" value="Raw"/>
0625	<KeyValue>
0626	<KeyMaterial type="ByteString"
	value="ef7833ab15f5a1ee5874bc0d9bbc4be7"/>
0627	</KeyValue>
0628	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0629	<CryptographicLength type="Integer" value="128"/>
0630	</KeyBlock>
0631	</SymmetricKey>
0632	</ResponsePayload>
0633	</BatchItem>
0634	</ResponseMessage>
	# TIME 14
0635	<RequestMessage>
0636	<RequestHeader>
0637	<ProtocolVersion>
0638	<ProtocolVersionMajor type="Integer" value="1"/>
0639	<ProtocolVersionMinor type="Integer" value="0"/>
0640	</ProtocolVersion>
0641	<BatchCount type="Integer" value="1"/>
0642	</RequestHeader>
0643	<BatchItem>
0644	<Operation type="Enumeration" value="Destroy"/>
0645	<RequestPayload>
0646	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0647	</RequestPayload>

0648	</BatchItem>
0649	</RequestMessage>
0650	<ResponseMessage>
0651	<ResponseHeader>
0652	<ProtocolVersion>
0653	<ProtocolVersionMajor type="Integer" value="1"/>
0654	<ProtocolVersionMinor type="Integer" value="0"/>
0655	</ProtocolVersion>
0656	<TimeStamp type="DateTime" value="2009-11-12T11:10:38+00:00"/>
0657	<BatchCount type="Integer" value="1"/>
0658	</ResponseHeader>
0659	<BatchItem>
0660	<Operation type="Enumeration" value="Destroy"/>
0661	<ResultStatus type="Enumeration" value="Success"/>
0662	<ResponsePayload>
0663	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0664	</ResponsePayload>
0665	</BatchItem>
0666	</ResponseMessage>

101

102 2.1.8 TC-51-10 - Get Usage Allocation Scenario

103 This test case tests the usage management functionality of KMIP. A key is created and the
104 Activation Date and Protect Stop Date attributes are set in such a way as to allow the Get Usage
105 Allocation operation to be performed. The value of the Usage Limits attribute is set to 1000
106 bytes, and two subsequent requests for 500 bytes succeed (one of them also verifying the
107 amount that can be received using the Check operation), while a third fails since the usage
108 allocation has been used up. The key is finally revoked and destroyed. This test case shows the
109 use of multiple clients (Client-A, Client-B and Client-C).

	# TIME 0
	# [Client-A]
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic

0020	Length"/>
0021	<AttributeValue type="Integer" value="128"/>
0022	</Attribute>
0023	<Attribute>
0024	<AttributeName type="TextString" value="Name"/>
0025	<AttributeValue>
0026	<NameValue type="TextString" value="Key1"/>
0027	<NameType type="Enumeration"
0028	value="UninterpretedTextString"/>
0029	</Attribute>
0030	<Attribute>
0031	<AttributeName type="TextString" value="Cryptographic
0032	Usage Mask"/>
0033	<AttributeValue type="Integer" value="Encrypt"/>
0034	</Attribute>
0035	</TemplateAttribute>
0036	</RequestPayload>
0037	</BatchItem>
0038	</RequestMessage>
0039	<ResponseMessage>
0040	<ResponseHeader>
0041	<ProtocolVersion>
0042	<ProtocolVersionMajor type="Integer" value="1"/>
0043	<ProtocolVersionMinor type="Integer" value="0"/>
0044	</ProtocolVersion>
0045	<TimeStamp type="DateTime" value="2010-03-11T12:21:46+00:00"/>
0046	<BatchCount type="Integer" value="1"/>
0047	</ResponseHeader>
0048	<BatchItem>
0049	<Operation type="Enumeration" value="Create"/>
0050	<ResultStatus type="Enumeration" value="Success"/>
0051	<ResponsePayload>
0052	<ObjectType type="Enumeration" value="SymmetricKey"/>
0053	<UniqueIdentifier type="TextString"
0054	value="\$UNIQUE_IDENTIFIER_0"/>
0055	</ResponsePayload>
0056	</BatchItem>
0057	</ResponseMessage>
0058	# TIME 1
0059	# [Client-A]
0060	<RequestMessage>
0061	<RequestHeader>
0062	<ProtocolVersion>
0063	<ProtocolVersionMajor type="Integer" value="1"/>
0064	<ProtocolVersionMinor type="Integer" value="0"/>
0065	</ProtocolVersion>
0066	<BatchCount type="Integer" value="2"/>
0067	</RequestHeader>
0068	<BatchItem>
0069	<Operation type="Enumeration" value="AddAttribute"/>
0070	<UniqueBatchItemID type="ByteString" value="d7fe2477e364ae1a"/>
0071	<RequestPayload>
0072	<UniqueIdentifier type="TextString"
0073	value="\$UNIQUE_IDENTIFIER_0"/>
0074	<Attribute>
0075	<AttributeName type="TextString" value="Activation Date"/>

0070	<AttributeValue type="DateTime" value="\$NOW-3600"/>
0071	</Attribute>
0072	</RequestPayload>
0073	</BatchItem>
0074	<BatchItem>
0075	<Operation type="Enumeration" value="AddAttribute"/>
0076	<UniqueBatchItemID type="ByteString" value="9696012991bc8a59"/>
0077	<RequestPayload>
0078	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0079	<Attribute>
0080	<AttributeName type="TextString" value="Protect Stop Date"/>
0081	<AttributeValue type="DateTime" value="\$NOW+600"/>
0082	</Attribute>
0083	</RequestPayload>
0084	</BatchItem>
0085	</RequestMessage>
0086	<ResponseMessage>
0087	<ResponseHeader>
0088	<ProtocolVersion>
0089	<ProtocolVersionMajor type="Integer" value="1"/>
0090	<ProtocolVersionMinor type="Integer" value="0"/>
0091	</ProtocolVersion>
0092	<TimeStamp type="DateTime" value="2010-03-11T12:21:47+00:00"/>
0093	<BatchCount type="Integer" value="2"/>
0094	</ResponseHeader>
0095	<BatchItem>
0096	<Operation type="Enumeration" value="AddAttribute"/>
0097	<UniqueBatchItemID type="ByteString" value="d7fe2477e364ae1a"/>
0098	<ResultStatus type="Enumeration" value="Success"/>
0099	<ResponsePayload>
0100	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0101	<Attribute>
0102	<AttributeName type="TextString" value="Activation Date"/>
0103	<AttributeValue type="DateTime" value="\$NOW-3600"/>
0104	</Attribute>
0105	</ResponsePayload>
0106	</BatchItem>
0107	<BatchItem>
0108	<Operation type="Enumeration" value="AddAttribute"/>
0109	<UniqueBatchItemID type="ByteString" value="9696012991bc8a59"/>
0110	<ResultStatus type="Enumeration" value="Success"/>
0111	<ResponsePayload>
0112	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0113	<Attribute>
0114	<AttributeName type="TextString" value="Protect Stop Date"/>
0115	<AttributeValue type="DateTime" value="\$NOW+600"/>
0116	</Attribute>
0117	</ResponsePayload>
0118	</BatchItem>
0119	</ResponseMessage>
	# TIME 2
	# [Client-A]
0120	<RequestMessage>
0121	<RequestHeader>

0122	<ProtocolVersion>
0123	<ProtocolVersionMajor type="Integer" value="1"/>
0124	<ProtocolVersionMinor type="Integer" value="0"/>
0125	</ProtocolVersion>
0126	<BatchCount type="Integer" value="1"/>
0127	</RequestHeader>
0128	<BatchItem>
0129	<Operation type="Enumeration" value="AddAttribute"/>
0130	<RequestPayload>
0131	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0132	<Attribute>
0133	<AttributeName type="TextString" value="Usage Limits"/>
0134	<AttributeValue>
0135	<UsageLimitsTotal type="LongInteger" value="1000"/>
0136	<UsageLimitsUnit type="Enumeration" value="Byte"/>
0137	</AttributeValue>
0138	</Attribute>
0139	</RequestPayload>
0140	</BatchItem>
0141	</RequestMessage>
0142	<ResponseMessage>
0143	<ResponseHeader>
0144	<ProtocolVersion>
0145	<ProtocolVersionMajor type="Integer" value="1"/>
0146	<ProtocolVersionMinor type="Integer" value="0"/>
0147	</ProtocolVersion>
0148	<TimeStamp type="DateTime" value="2010-03-11T12:21:48+00:00"/>
0149	<BatchCount type="Integer" value="1"/>
0150	</ResponseHeader>
0151	<BatchItem>
0152	<Operation type="Enumeration" value="AddAttribute"/>
0153	<ResultStatus type="Enumeration" value="Success"/>
0154	<ResponsePayload>
0155	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0156	<Attribute>
0157	<AttributeName type="TextString" value="Usage Limits"/>
0158	<AttributeValue>
0159	<UsageLimitsTotal type="LongInteger" value="1000"/>
0160	<UsageLimitsCount type="LongInteger" value="1000"/>
0161	<UsageLimitsUnit type="Enumeration" value="Byte"/>
0162	</AttributeValue>
0163	</Attribute>
0164	</ResponsePayload>
0165	</BatchItem>
0166	</ResponseMessage>
	# TIME 3
	# [Client-B]
0167	<RequestMessage>
0168	<RequestHeader>
0169	<ProtocolVersion>
0170	<ProtocolVersionMajor type="Integer" value="1"/>
0171	<ProtocolVersionMinor type="Integer" value="0"/>
0172	</ProtocolVersion>
0173	<BatchCount type="Integer" value="1"/>
0174	</RequestHeader>

0175	<BatchItem>
0176	<Operation type="Enumeration" value="Locate"/>
0177	<RequestPayload>
0178	<Attribute>
0179	<AttributeName type="TextString" value="Object Type"/>
0180	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0181	</Attribute>
0182	<Attribute>
0183	<AttributeName type="TextString" value="Name"/>
0184	<AttributeValue>
0185	<NameValue type="TextString" value="Key1"/>
0186	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0187	</AttributeValue>
0188	</Attribute>
0189	</RequestPayload>
0190	</BatchItem>
0191	</RequestMessage>
0192	<ResponseMessage>
0193	<ResponseHeader>
0194	<ProtocolVersion>
0195	<ProtocolVersionMajor type="Integer" value="1"/>
0196	<ProtocolVersionMinor type="Integer" value="0"/>
0197	</ProtocolVersion>
0198	<TimeStamp type="DateTime" value="2010-03-11T12:21:48+00:00"/>
0199	<BatchCount type="Integer" value="1"/>
0200	</ResponseHeader>
0201	<BatchItem>
0202	<Operation type="Enumeration" value="Locate"/>
0203	<ResultStatus type="Enumeration" value="Success"/>
0204	<ResponsePayload>
0205	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0206	</ResponsePayload>
0207	</BatchItem>
0208	</ResponseMessage>
0209	# TIME 4
0210	# [Client-B]
0210	<RequestMessage>
0211	<RequestHeader>
0212	<ProtocolVersion>
0213	<ProtocolVersionMajor type="Integer" value="1"/>
0214	<ProtocolVersionMinor type="Integer" value="0"/>
0215	</ProtocolVersion>
0216	<BatchCount type="Integer" value="1"/>
0217	</RequestHeader>
0218	<BatchItem>
0219	<Operation type="Enumeration" value="Get"/>
0220	<RequestPayload>
0221	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0222	</RequestPayload>
0223	</BatchItem>
0224	</RequestMessage>
0225	<ResponseMessage>
	<ResponseHeader>

0226	<ProtocolVersion>
0227	<ProtocolVersionMajor type="Integer" value="1"/>
0228	<ProtocolVersionMinor type="Integer" value="0"/>
0229	</ProtocolVersion>
0230	<TimeStamp type="DateTime" value="2010-03-11T12:21:48+00:00"/>
0231	<BatchCount type="Integer" value="1"/>
0232	</ResponseHeader>
0233	<BatchItem>
0234	<Operation type="Enumeration" value="Get"/>
0235	<ResultStatus type="Enumeration" value="Success"/>
0236	<ResponsePayload>
0237	<ObjectType type="Enumeration" value="SymmetricKey"/>
0238	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0239	<SymmetricKey>
0240	<KeyBlock>
0241	<KeyFormatType type="Enumeration" value="Raw"/>
0242	<KeyValue>
0243	<KeyMaterial type="ByteString"
	value="674b32b1a3266df1253b0f2c4440b0b0"/>
0244	</KeyValue>
0245	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0246	<CryptographicLength type="Integer" value="128"/>
0247	</KeyBlock>
0248	</SymmetricKey>
0249	</ResponsePayload>
0250	</BatchItem>
0251	</ResponseMessage>
	# TIME 5
	# [Client-B]
0252	<RequestMessage>
0253	<RequestHeader>
0254	<ProtocolVersion>
0255	<ProtocolVersionMajor type="Integer" value="1"/>
0256	<ProtocolVersionMinor type="Integer" value="0"/>
0257	</ProtocolVersion>
0258	<BatchOrderOption type="Boolean" value="true"/>
0259	<BatchCount type="Integer" value="2"/>
0260	</RequestHeader>
0261	<BatchItem>
0262	<Operation type="Enumeration" value="Check"/>
0263	<UniqueBatchItemID type="ByteString" value="19d4f3dc9635307a"/>
0264	<RequestPayload>
0265	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0266	<UsageLimitsCount type="LongInteger" value="500"/>
0267	</RequestPayload>
0268	</BatchItem>
0269	<BatchItem>
0270	<Operation type="Enumeration" value="GetUsageAllocation"/>
0271	<UniqueBatchItemID type="ByteString" value="20c8dff55bdeee8"/>
0272	<RequestPayload>
0273	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0274	<UsageLimitsCount type="LongInteger" value="500"/>
0275	</RequestPayload>
0276	</BatchItem>

0277	</RequestMessage>
0278	<ResponseMessage>
0279	<ResponseHeader>
0280	<ProtocolVersion>
0281	<ProtocolVersionMajor type="Integer" value="1"/>
0282	<ProtocolVersionMinor type="Integer" value="0"/>
0283	</ProtocolVersion>
0284	<TimeStamp type="DateTime" value="2010-03-11T12:21:49+00:00"/>
0285	<BatchCount type="Integer" value="2"/>
0286	</ResponseHeader>
0287	<BatchItem>
0288	<Operation type="Enumeration" value="Check"/>
0289	<UniqueBatchItemID type="ByteString" value="19d4f3dc9635307a"/>
0290	<ResultStatus type="Enumeration" value="Success"/>
0291	<ResponsePayload>
0292	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0293	</ResponsePayload>
0294	</BatchItem>
0295	<BatchItem>
0296	<Operation type="Enumeration" value="GetUsageAllocation"/>
0297	<UniqueBatchItemID type="ByteString" value="20c8dfffd55bdeee8"/>
0298	<ResultStatus type="Enumeration" value="Success"/>
0299	<ResponsePayload>
0300	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0301	</ResponsePayload>
0302	</BatchItem>
0303	</ResponseMessage>
	# TIME 6
	# [Client-A]
0304	<RequestMessage>
0305	<RequestHeader>
0306	<ProtocolVersion>
0307	<ProtocolVersionMajor type="Integer" value="1"/>
0308	<ProtocolVersionMinor type="Integer" value="0"/>
0309	</ProtocolVersion>
0310	<BatchCount type="Integer" value="1"/>
0311	</RequestHeader>
0312	<BatchItem>
0313	<Operation type="Enumeration" value="GetUsageAllocation"/>
0314	<RequestPayload>
0315	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0316	<UsageLimitsCount type="LongInteger" value="500"/>
0317	</RequestPayload>
0318	</BatchItem>
0319	</RequestMessage>
0320	<ResponseMessage>
0321	<ResponseHeader>
0322	<ProtocolVersion>
0323	<ProtocolVersionMajor type="Integer" value="1"/>
0324	<ProtocolVersionMinor type="Integer" value="0"/>
0325	</ProtocolVersion>
0326	<TimeStamp type="DateTime" value="2010-03-11T12:21:49+00:00"/>
0327	<BatchCount type="Integer" value="1"/>

0328	</ResponseHeader>
0329	<BatchItem>
0330	<Operation type="Enumeration" value="GetUsageAllocation"/>
0331	<ResultStatus type="Enumeration" value="Success"/>
0332	<ResponsePayload>
0333	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0334	</ResponsePayload>
0335	</BatchItem>
0336	</ResponseMessage>
	# TIME 7
	# [Client-C]
0337	<RequestMessage>
0338	<RequestHeader>
0339	<ProtocolVersion>
0340	<ProtocolVersionMajor type="Integer" value="1"/>
0341	<ProtocolVersionMinor type="Integer" value="0"/>
0342	</ProtocolVersion>
0343	<BatchCount type="Integer" value="1"/>
0344	</RequestHeader>
0345	<BatchItem>
0346	<Operation type="Enumeration" value="Locate"/>
0347	<RequestPayload>
0348	<Attribute>
0349	<AttributeName type="TextString" value="Object Type"/>
0350	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0351	</Attribute>
0352	<Attribute>
0353	<AttributeName type="TextString" value="Name"/>
0354	<AttributeValue>
0355	<NameValue type="TextString" value="Key1"/>
0356	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0357	</AttributeValue>
0358	</Attribute>
0359	</RequestPayload>
0360	</BatchItem>
0361	</RequestMessage>
0362	<ResponseMessage>
0363	<ResponseHeader>
0364	<ProtocolVersion>
0365	<ProtocolVersionMajor type="Integer" value="1"/>
0366	<ProtocolVersionMinor type="Integer" value="0"/>
0367	</ProtocolVersion>
0368	<TimeStamp type="DateTime" value="2010-03-11T12:21:49+00:00"/>
0369	<BatchCount type="Integer" value="1"/>
0370	</ResponseHeader>
0371	<BatchItem>
0372	<Operation type="Enumeration" value="Locate"/>
0373	<ResultStatus type="Enumeration" value="Success"/>
0374	<ResponsePayload>
0375	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0376	</ResponsePayload>
0377	</BatchItem>
0378	</ResponseMessage>

0379	# TIME 8
0380	# [Client-C]
0381	<RequestMessage>
0382	<RequestHeader>
0383	<ProtocolVersion>
0384	<ProtocolVersionMajor type="Integer" value="1"/>
0385	<ProtocolVersionMinor type="Integer" value="0"/>
0386	</ProtocolVersion>
0387	<BatchCount type="Integer" value="1"/>
0388	</BatchCount>
0389	<Operation type="Enumeration" value="Get"/>
0390	<RequestPayload>
0391	<UniqueIdentifier type="TextString"
0392	value="\$UNIQUE_IDENTIFIER_0"/>
0393	</UniqueIdentifier>
0394	</RequestPayload>
0395	</BatchItem>
0396	</RequestMessage>
0397	<ResponseMessage>
0398	<ResponseHeader>
0399	<ProtocolVersion>
0400	<ProtocolVersionMajor type="Integer" value="1"/>
0401	<ProtocolVersionMinor type="Integer" value="0"/>
0402	</ProtocolVersion>
0403	<TimeStamp type="DateTime" value="2010-03-11T12:21:49+00:00"/>
0404	<BatchCount type="Integer" value="1"/>
0405	</BatchCount>
0406	<Operation type="Enumeration" value="Get"/>
0407	<ResultStatus type="Enumeration" value="Success"/>
0408	<ResponsePayload>
0409	<ObjectType type="Enumeration" value="SymmetricKey"/>
0410	<UniqueIdentifier type="TextString"
0411	value="\$UNIQUE_IDENTIFIER_0"/>
0412	</UniqueIdentifier>
0413	<SymmetricKey>
0414	<KeyBlock>
0415	<KeyFormatType type="Enumeration" value="Raw"/>
0416	<KeyValue>
0417	<KeyMaterial type="ByteString"
0418	value="674b32b1a3266df1253b0f2c4440b0b0"/>
0419	</KeyMaterial>
0420	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0421	<CryptographicLength type="Integer" value="128"/>
0422	</CryptographicLength>
0423	</KeyBlock>
0424	</SymmetricKey>
0425	</ResponsePayload>
0426	</BatchItem>
0427	</ResponseMessage>
0428	# TIME 9
	# [Client-C]
0429	<RequestMessage>
0430	<RequestHeader>
0431	<ProtocolVersion>
0432	<ProtocolVersionMajor type="Integer" value="1"/>
0433	<ProtocolVersionMinor type="Integer" value="0"/>
0434	</ProtocolVersion>
0435	<BatchCount type="Integer" value="1"/>

0429	</RequestHeader>
0430	<BatchItem>
0431	<Operation type="Enumeration" value="GetUsageAllocation"/>
0432	<RequestPayload>
0433	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0434	<UsageLimitsCount type="LongInteger" value="500"/>
0435	</RequestPayload>
0436	</BatchItem>
0437	</RequestMessage>
0438	<ResponseMessage>
0439	<ResponseHeader>
0440	<ProtocolVersion>
0441	<ProtocolVersionMajor type="Integer" value="1"/>
0442	<ProtocolVersionMinor type="Integer" value="0"/>
0443	</ProtocolVersion>
0444	<TimeStamp type="DateTime" value="2010-03-11T12:21:49+00:00"/>
0445	<BatchCount type="Integer" value="1"/>
0446	</ResponseHeader>
0447	<BatchItem>
0448	<Operation type="Enumeration" value="GetUsageAllocation"/>
0449	<ResultStatus type="Enumeration" value="OperationFailed"/>
0450	<ResultReason type="Enumeration" value="PermissionDenied"/>
0451	<ResultMessage type="TextString" value="Unable to allocate
	requested amount"/>
0452	</BatchItem>
0453	</ResponseMessage>
	# TIME 10
	# [Client-A]
0454	<RequestMessage>
0455	<RequestHeader>
0456	<ProtocolVersion>
0457	<ProtocolVersionMajor type="Integer" value="1"/>
0458	<ProtocolVersionMinor type="Integer" value="0"/>
0459	</ProtocolVersion>
0460	<BatchOrderOption type="Boolean" value="true"/>
0461	<BatchCount type="Integer" value="2"/>
0462	</RequestHeader>
0463	<BatchItem>
0464	<Operation type="Enumeration" value="Revoke"/>
0465	<UniqueBatchItemID type="ByteString" value="727a212bc674b4ea"/>
0466	<RequestPayload>
0467	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0468	<RevocationReason>
0469	<RevocationReasonCode type="Enumeration"
	value="CessationOfOperation"/>
0470	</RevocationReason>
0471	</RequestPayload>
0472	</BatchItem>
0473	<BatchItem>
0474	<Operation type="Enumeration" value="Destroy"/>
0475	<UniqueBatchItemID type="ByteString" value="1d0ebf826109b0a5"/>
0476	<RequestPayload>
0477	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0478	</RequestPayload>

```

0479     </BatchItem>
0480 </RequestMessage>
0481 <ResponseMessage>
0482   <ResponseHeader>
0483     <ProtocolVersion>
0484       <ProtocolVersionMajor type="Integer" value="1"/>
0485       <ProtocolVersionMinor type="Integer" value="0"/>
0486     </ProtocolVersion>
0487     <TimeStamp type="DateTime" value="2010-03-11T12:21:51+00:00"/>
0488     <BatchCount type="Integer" value="2"/>
0489   </ResponseHeader>
0490   <BatchItem>
0491     <Operation type="Enumeration" value="Revoke"/>
0492     <UniqueBatchItemID type="ByteString" value="727a212bc674b4ea"/>
0493     <ResultStatus type="Enumeration" value="Success"/>
0494     <ResponsePayload>
0495       <UniqueIdentifier type="TextString"
0496       value="$UNIQUE_IDENTIFIER_0"/>
0497     </ResponsePayload>
0498   </BatchItem>
0499   <BatchItem>
0500     <Operation type="Enumeration" value="Destroy"/>
0501     <UniqueBatchItemID type="ByteString" value="1d0ebf826109b0a5"/>
0502     <ResultStatus type="Enumeration" value="Success"/>
0503     <ResponsePayload>
0504       <UniqueIdentifier type="TextString"
0505       value="$UNIQUE_IDENTIFIER_0"/>
0506     </ResponsePayload>
0507   </BatchItem>
0508 </ResponseMessage>

```

110

111 2.1.9 TC-61-10 - Import of a Third-party Key

112 This test case tests the import of a foreign key using the Register operation. To validate that the
113 registered key is treated the same as a locally created key, an attribute is added to the key and
114 then modified. Finally, the key is destroyed.

```

0001 # TIME 0
0002 <RequestMessage>
0003   <RequestHeader>
0004     <ProtocolVersion>
0005       <ProtocolVersionMajor type="Integer" value="1"/>
0006       <ProtocolVersionMinor type="Integer" value="0"/>
0007     </ProtocolVersion>
0008     <BatchCount type="Integer" value="1"/>
0009   </RequestHeader>
0010   <BatchItem>
0011     <Operation type="Enumeration" value="Register"/>
0012     <RequestPayload>
0013       <ObjectType type="Enumeration" value="SymmetricKey"/>
0014       <TemplateAttribute>
0015         <Attribute>
0016           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0017           <AttributeValue type="Integer" value="Encrypt"/>

```


0017	</Attribute>
0018	</TemplateAttribute>
0019	<SymmetricKey>
0020	<KeyBlock>
0021	<KeyFormatType type="Enumeration" value="Raw"/>
0022	<KeyValue>
0023	<KeyMaterial type="ByteString"
	value="0123456789abcdef0123456789abcdef"/>
0024	</KeyValue>
0025	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0026	<CryptographicLength type="Integer" value="128"/>
0027	</KeyBlock>
0028	</SymmetricKey>
0029	</RequestPayload>
0030	</BatchItem>
0031	</RequestMessage>
0032	<ResponseMessage>
0033	<ResponseHeader>
0034	<ProtocolVersion>
0035	<ProtocolVersionMajor type="Integer" value="1"/>
0036	<ProtocolVersionMinor type="Integer" value="0"/>
0037	</ProtocolVersion>
0038	<TimeStamp type="DateTime" value="2009-11-12T11:10:42+00:00"/>
0039	<BatchCount type="Integer" value="1"/>
0040	</ResponseHeader>
0041	<BatchItem>
0042	<Operation type="Enumeration" value="Register"/>
0043	<ResultStatus type="Enumeration" value="Success"/>
0044	<ResponsePayload>
0045	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0046	</ResponsePayload>
0047	</BatchItem>
0048	</ResponseMessage>
	# TIME 1
0049	<RequestMessage>
0050	<RequestHeader>
0051	<ProtocolVersion>
0052	<ProtocolVersionMajor type="Integer" value="1"/>
0053	<ProtocolVersionMinor type="Integer" value="0"/>
0054	</ProtocolVersion>
0055	<BatchCount type="Integer" value="1"/>
0056	</RequestHeader>
0057	<BatchItem>
0058	<Operation type="Enumeration" value="AddAttribute"/>
0059	<RequestPayload>
0060	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0061	<Attribute>
0062	<AttributeName type="TextString" value="x-provider"/>
0063	<AttributeValue type="TextString" value="unknown"/>
0064	</Attribute>
0065	</RequestPayload>
0066	</BatchItem>
0067	</RequestMessage>
0068	<ResponseMessage>

0069	<ResponseHeader>
0070	<ProtocolVersion>
0071	<ProtocolVersionMajor type="Integer" value="1"/>
0072	<ProtocolVersionMinor type="Integer" value="0"/>
0073	</ProtocolVersion>
0074	<TimeStamp type="DateTime" value="2009-11-12T11:10:42+00:00"/>
0075	<BatchCount type="Integer" value="1"/>
0076	</ResponseHeader>
0077	<BatchItem>
0078	<Operation type="Enumeration" value="AddAttribute"/>
0079	<ResultStatus type="Enumeration" value="Success"/>
0080	<ResponsePayload>
0081	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0082	<Attribute>
0083	<AttributeName type="TextString" value="x-provider"/>
0084	<AttributeValue type="TextString" value="unknown"/>
0085	</Attribute>
0086	</ResponsePayload>
0087	</BatchItem>
0088	</ResponseMessage>
# TIME 2	
0089	<RequestMessage>
0090	<RequestHeader>
0091	<ProtocolVersion>
0092	<ProtocolVersionMajor type="Integer" value="1"/>
0093	<ProtocolVersionMinor type="Integer" value="0"/>
0094	</ProtocolVersion>
0095	<BatchCount type="Integer" value="1"/>
0096	</RequestHeader>
0097	<BatchItem>
0098	<Operation type="Enumeration" value="ModifyAttribute"/>
0099	<RequestPayload>
0100	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0101	<Attribute>
0102	<AttributeName type="TextString" value="x-provider"/>
0103	<AttributeValue type="TextString" value="third party"/>
0104	</Attribute>
0105	</RequestPayload>
0106	</BatchItem>
0107	</RequestMessage>
0108	<ResponseMessage>
0109	<ResponseHeader>
0110	<ProtocolVersion>
0111	<ProtocolVersionMajor type="Integer" value="1"/>
0112	<ProtocolVersionMinor type="Integer" value="0"/>
0113	</ProtocolVersion>
0114	<TimeStamp type="DateTime" value="2009-11-12T11:10:42+00:00"/>
0115	<BatchCount type="Integer" value="1"/>
0116	</ResponseHeader>
0117	<BatchItem>
0118	<Operation type="Enumeration" value="ModifyAttribute"/>
0119	<ResultStatus type="Enumeration" value="Success"/>
0120	<ResponsePayload>
0121	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0122	<Attribute>
0123	<AttributeName type="TextString" value="x-provider"/>
0124	<AttributeValue type="TextString" value="third party"/>
0125	</Attribute>
0126	</ResponsePayload>
0127	</BatchItem>
0128	</ResponseMessage>
# TIME 3	
0129	<RequestMessage>
0130	<RequestHeader>
0131	<ProtocolVersion>
0132	<ProtocolVersionMajor type="Integer" value="1"/>
0133	<ProtocolVersionMinor type="Integer" value="0"/>
0134	</ProtocolVersion>
0135	<BatchCount type="Integer" value="1"/>
0136	</RequestHeader>
0137	<BatchItem>
0138	<Operation type="Enumeration" value="Destroy"/>
0139	<RequestPayload>
0140	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0141	</RequestPayload>
0142	</BatchItem>
0143	</RequestMessage>
0144	<ResponseMessage>
0145	<ResponseHeader>
0146	<ProtocolVersion>
0147	<ProtocolVersionMajor type="Integer" value="1"/>
0148	<ProtocolVersionMinor type="Integer" value="0"/>
0149	</ProtocolVersion>
0150	<TimeStamp type="DateTime" value="2009-11-12T11:10:42+00:00"/>
0151	<BatchCount type="Integer" value="1"/>
0152	</ResponseHeader>
0153	<BatchItem>
0154	<Operation type="Enumeration" value="Destroy"/>
0155	<ResultStatus type="Enumeration" value="Success"/>
0156	<ResponsePayload>
0157	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0158	</ResponsePayload>
0159	</BatchItem>
0160	</ResponseMessage>

115

116 2.1.10 TC-71-10 - Unrecognized Message Extension with Criticality Indicator

117 False

118 A create request is issued and the request contains a Message Extension with the Criticality
119 Indicator set to false. The server does not understand the extension, but since it is non-critical,
120 the create request is processed normally. Subsequently, the created key is deleted.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>

0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Length"/>
0017	<AttributeValue type="Integer" value="128"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Algorithm"/>
0022	<AttributeValue type="Enumeration" value="AES"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Cryptographic
0026	Usage Mask"/>
0027	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="x-ID"/>
0031	<AttributeValue type="TextString" value="TC-71-10"/>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	<MessageExtension>
0036	<VendorIdentification type="TextString" value="Acme"/>
0037	<CriticalityIndicator type="Boolean" value="false"/>
0038	<VendorExtension>
0039	<TLV tag="0x540001" type="TextString" value="na"/>
0040	</VendorExtension>
0041	</MessageExtension>
0042	</BatchItem>
0043	</RequestMessage>
0044	<ResponseMessage>
0045	<ResponseHeader>
0046	<ProtocolVersion>
0047	<ProtocolVersionMajor type="Integer" value="1"/>
0048	<ProtocolVersionMinor type="Integer" value="0"/>
0049	</ProtocolVersion>
0050	<TimeStamp type="DateTime" value="2010-02-11T08:26:04+00:00"/>
0051	<BatchCount type="Integer" value="1"/>
0052	</ResponseHeader>
0053	<BatchItem>
0054	<Operation type="Enumeration" value="Create"/>
0055	<ResultStatus type="Enumeration" value="Success"/>
0056	<ResponsePayload>
0057	<ObjectType type="Enumeration" value="SymmetricKey"/>
0058	<UniqueIdentifier type="TextString"
0059	value="\$UNIQUE_IDENTIFIER_0"/>
0060	</ResponsePayload>

0057	</BatchItem>
0058	</ResponseMessage>
# TIME 1	
0059	<RequestMessage>
0060	<RequestHeader>
0061	<ProtocolVersion>
0062	<ProtocolVersionMajor type="Integer" value="1"/>
0063	<ProtocolVersionMinor type="Integer" value="0"/>
0064	</ProtocolVersion>
0065	<BatchCount type="Integer" value="1"/>
0066	</RequestHeader>
0067	<BatchItem>
0068	<Operation type="Enumeration" value="Destroy"/>
0069	<RequestPayload>
0070	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0071	</RequestPayload>
0072	</BatchItem>
0073	</RequestMessage>
0074	<ResponseMessage>
0075	<ResponseHeader>
0076	<ProtocolVersion>
0077	<ProtocolVersionMajor type="Integer" value="1"/>
0078	<ProtocolVersionMinor type="Integer" value="0"/>
0079	</ProtocolVersion>
0080	<TimeStamp type="DateTime" value="2010-02-11T08:26:04+00:00"/>
0081	<BatchCount type="Integer" value="1"/>
0082	</ResponseHeader>
0083	<BatchItem>
0084	<Operation type="Enumeration" value="Destroy"/>
0085	<ResultStatus type="Enumeration" value="Success"/>
0086	<ResponsePayload>
0087	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0088	</ResponsePayload>
0089	</BatchItem>
0090	</ResponseMessage>

121

122 2.1.11 TC-72-10 - Unrecognized Message Extension with Criticality Indicator 123 True

124 A create request is issued and the request contains a Message Extension with the Criticality
125 Indicator set to true. The server does not understand the extension, and since it is critical, the
126 create request fails and an error is returned.

# TIME 0	
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>

0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Length"/>
0017	<AttributeValue type="Integer" value="128"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Algorithm"/>
0022	<AttributeValue type="Enumeration" value="AES"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Cryptographic
0026	Usage Mask"/>
0027	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="x-ID"/>
0031	<AttributeValue type="TextString" value="TC-72-10"/>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	<MessageExtension>
0036	<VendorIdentification type="TextString" value="Acme"/>
0037	<CriticalityIndicator type="Boolean" value="true"/>
0038	<VendorExtension>
0039	<TTLV tag="0x540001" type="TextString" value="na"/>
0040	</VendorExtension>
0041	</MessageExtension>
0042	</BatchItem>
0043	</RequestMessage>
0044	<ResponseMessage>
0045	<ResponseHeader>
0046	<ProtocolVersion>
0047	<ProtocolVersionMajor type="Integer" value="1"/>
0048	<ProtocolVersionMinor type="Integer" value="0"/>
0049	</ProtocolVersion>
0050	<TimeStamp type="DateTime" value="2010-02-11T08:26:05+00:00"/>
0051	<BatchCount type="Integer" value="1"/>
0052	</ResponseHeader>
0053	<BatchItem>
0054	<Operation type="Enumeration" value="Create"/>
0055	<ResultStatus type="Enumeration" value="OperationFailed"/>
0056	<ResultReason type="Enumeration" value="FeatureNotSupported"/>
0057	<ResultMessage type="TextString" value="Critical Message
0058	Extension not recognized"/>
0059	</BatchItem>
0060	</ResponseMessage>

128 2.1.12 TC-81-10 - Create a Key Pair

- 129 Create a new private/public key pair. Make sure they are linked correctly by issuing Locate
130 commands with the assigned Unique Identifiers. Finally delete both key halves.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="CreateKeyPair"/>
0011	<RequestPayload>
0012	<CommonTemplateAttribute>
0013	<Attribute>
0014	<AttributeName type="TextString" value="Cryptographic
0015	Algorithm"/>
0016	<AttributeValue type="Enumeration" value="RSA"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
0020	Length"/>
0021	<AttributeValue type="Integer" value="1024"/>
0022	</Attribute>
0023	</CommonTemplateAttribute>
0024	<PrivateKeyTemplateAttribute>
0025	<Attribute>
0026	<AttributeName type="TextString" value="Name"/>
0027	<AttributeValue>
0028	<NameValue type="TextString" value="PrivateKey1"/>
0029	<NameType type="Enumeration"
0030	value="UninterpretedTextString"/>
0031	</AttributeValue>
0032	</Attribute>
0033	<Attribute>
0034	<AttributeName type="TextString" value="Cryptographic
0035	Usage Mask"/>
0036	<AttributeValue type="Integer" value="Sign"/>
0037	</Attribute>
0038	</PrivateKeyTemplateAttribute>
0039	<PublicKeyTemplateAttribute>
0040	<Attribute>
0041	<AttributeName type="TextString" value="Name"/>
0042	<AttributeValue>
0043	<NameValue type="TextString" value="PublicKey1"/>
0044	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
	</AttributeValue>
	</Attribute>
	</PublicKeyTemplateAttribute>
	</BatchItem>
	</Batch>
	</RequestPayload>
	</RequestMessage>

0045	<AttributeValue type="Integer" value="Verify"/>
0046	</Attribute>
0047	</PublicKeyTemplateAttribute>
0048	</RequestPayload>
0049	</BatchItem>
0050	</RequestMessage>
0051	<ResponseMessage>
0052	<ResponseHeader>
0053	<ProtocolVersion>
0054	<ProtocolVersionMajor type="Integer" value="1"/>
0055	<ProtocolVersionMinor type="Integer" value="0"/>
0056	</ProtocolVersion>
0057	<TimeStamp type="DateTime" value="2010-02-11T08:35:06+00:00"/>
0058	<BatchCount type="Integer" value="1"/>
0059	</ResponseHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="CreateKeyPair"/>
0062	<ResultStatus type="Enumeration" value="Success"/>
0063	<ResponsePayload>
0064	<PrivateKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0065	<PublicKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
0069	# TIME 1
0070	<RequestMessage>
0071	<RequestHeader>
0072	<ProtocolVersion>
0073	<ProtocolVersionMajor type="Integer" value="1"/>
0074	<ProtocolVersionMinor type="Integer" value="0"/>
0075	</ProtocolVersion>
0076	<BatchCount type="Integer" value="1"/>
0077	</RequestHeader>
0078	<BatchItem>
0079	<Operation type="Enumeration" value="Locate"/>
0080	<RequestPayload>
0081	<Attribute>
0082	<AttributeName type="TextString" value="Object Type"/>
0083	<AttributeValue type="Enumeration" value="PublicKey"/>
0084	</Attribute>
0085	<Attribute>
0086	<AttributeName type="TextString" value="Link"/>
0087	<AttributeValue>
0088	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0089	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0090	</Attribute>
0091	</RequestPayload>
0092	</BatchItem>
0093	</RequestMessage>
0094	<ResponseMessage>
0095	<ResponseHeader>
0096	<ProtocolVersion>

0097	<ProtocolVersionMajor type="Integer" value="1"/>
0098	<ProtocolVersionMinor type="Integer" value="0"/>
0099	</ProtocolVersion>
0100	<TimeStamp type="DateTime" value="2010-02-11T08:35:07+00:00"/>
0101	<BatchCount type="Integer" value="1"/>
0102	</ResponseHeader>
0103	<BatchItem>
0104	<Operation type="Enumeration" value="Locate"/>
0105	<ResultStatus type="Enumeration" value="Success"/>
0106	<ResponsePayload>
0107	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0108	</ResponsePayload>
0109	</BatchItem>
0110	</ResponseMessage>
# TIME 2	
0111	<RequestMessage>
0112	<RequestHeader>
0113	<ProtocolVersion>
0114	<ProtocolVersionMajor type="Integer" value="1"/>
0115	<ProtocolVersionMinor type="Integer" value="0"/>
0116	</ProtocolVersion>
0117	<BatchCount type="Integer" value="1"/>
0118	</RequestHeader>
0119	<BatchItem>
0120	<Operation type="Enumeration" value="Locate"/>
0121	<RequestPayload>
0122	<Attribute>
0123	<AttributeName type="TextString" value="Object Type"/>
0124	<AttributeValue type="Enumeration" value="PrivateKey"/>
0125	</Attribute>
0126	<Attribute>
0127	<AttributeName type="TextString" value="Link"/>
0128	<AttributeValue>
0129	<LinkType type="Enumeration" value="PublicKeyLink"/>
0130	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0131	</AttributeValue>
0132	</Attribute>
0133	</RequestPayload>
0134	</BatchItem>
0135	</RequestMessage>
0136	<ResponseMessage>
0137	<ResponseHeader>
0138	<ProtocolVersion>
0139	<ProtocolVersionMajor type="Integer" value="1"/>
0140	<ProtocolVersionMinor type="Integer" value="0"/>
0141	</ProtocolVersion>
0142	<TimeStamp type="DateTime" value="2010-02-11T08:35:07+00:00"/>
0143	<BatchCount type="Integer" value="1"/>
0144	</ResponseHeader>
0145	<BatchItem>
0146	<Operation type="Enumeration" value="Locate"/>
0147	<ResultStatus type="Enumeration" value="Success"/>
0148	<ResponsePayload>
0149	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0150	</ResponsePayload>
0151	</BatchItem>
0152	</ResponseMessage>
# TIME 3	
0153	<RequestMessage>
0154	<RequestHeader>
0155	<ProtocolVersion>
0156	<ProtocolVersionMajor type="Integer" value="1"/>
0157	<ProtocolVersionMinor type="Integer" value="0"/>
0158	</ProtocolVersion>
0159	<BatchCount type="Integer" value="1"/>
0160	</RequestHeader>
0161	<BatchItem>
0162	<Operation type="Enumeration" value="Destroy"/>
0163	<RequestPayload>
0164	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0165	</RequestPayload>
0166	</BatchItem>
0167	</RequestMessage>
0168	<ResponseMessage>
0169	<ResponseHeader>
0170	<ProtocolVersion>
0171	<ProtocolVersionMajor type="Integer" value="1"/>
0172	<ProtocolVersionMinor type="Integer" value="0"/>
0173	</ProtocolVersion>
0174	<TimeStamp type="DateTime" value="2010-02-11T08:35:07+00:00"/>
0175	<BatchCount type="Integer" value="1"/>
0176	</ResponseHeader>
0177	<BatchItem>
0178	<Operation type="Enumeration" value="Destroy"/>
0179	<ResultStatus type="Enumeration" value="Success"/>
0180	<ResponsePayload>
0181	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0182	</ResponsePayload>
0183	</BatchItem>
0184	</ResponseMessage>
# TIME 4	
0185	<RequestMessage>
0186	<RequestHeader>
0187	<ProtocolVersion>
0188	<ProtocolVersionMajor type="Integer" value="1"/>
0189	<ProtocolVersionMinor type="Integer" value="0"/>
0190	</ProtocolVersion>
0191	<BatchCount type="Integer" value="1"/>
0192	</RequestHeader>
0193	<BatchItem>
0194	<Operation type="Enumeration" value="Destroy"/>
0195	<RequestPayload>
0196	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0197	</RequestPayload>
0198	</BatchItem>
0199	</RequestMessage>
0200	<ResponseMessage>

0201	<ResponseHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="0"/>
0205	</ProtocolVersion>
0206	<TimeStamp type="DateTime" value="2010-02-11T08:35:07+00:00"/>
0207	<BatchCount type="Integer" value="1"/>
0208	</ResponseHeader>
0209	<BatchItem>
0210	<Operation type="Enumeration" value="Destroy"/>
0211	<ResultStatus type="Enumeration" value="Success"/>
0212	<ResponsePayload>
0213	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0214	</ResponsePayload>
0215	</BatchItem>
0216	</ResponseMessage>

131

132 2.1.13 TC-82-10 - Register Both Halves of a Key Pair

133 Register a private key and a public key and set the Link attribute to point to each other. Verify
134 the links were set correctly by locating the keys based on the link attributes, and then delete
135 both objects.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="PrivateKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0016	<AttributeValue type="Integer" value="Sign"/>
0017	</Attribute>
0018	</TemplateAttribute>
0019	<PrivateKey>
0020	<KeyBlock>
0021	<KeyFormatType type="Enumeration" value="PKCS_8"/>
0022	<KeyValue>
0023	<KeyMaterial type="ByteString"
	value="30820276020100300d06092a864886f70d0101010500048202603082025c0
	2010002818100930451c9ecd94f5bb9da17dd09381bd23be43eca8c7539f301fc8a8
	cd5d5274c3e7699dbdc711c97a7aa91e2c50a82bd0b1034f0df493dec16362427e58
	acce7f6ce0f9bcc617bbd8c90d0094a2703ba0d09eb19d1005f2fb265526aac75af3
	2f8bc782cded2a57f811e03eaf67a944de5e78413dca8f232d074e6dcea4cec9f020
	30100010281800b6a7d736199ea48a420e4537ca0c7c046784dcbeaa63baebc0bc13

	2787449cde8d7cad0c0c863c0fefb06c3062befc50033ecf87b4e33a9be7bcbcb8f1511ae215e80deb5d8af2bd31319d7821196640935a0cd67c94599579f2100d65e038831fdafb0dbe2bbdac00a696e67e756350e1c99ace11a36dabac3ed3e730960059024100ddf672fbcc5bda3d73affc4e791e0c03390224405d69ccaabc749faa0dcd4c2583c71dde8941a7b9aa030f52ef1451466c074d4d338fe677892acd9e10fd35bd024100a98fbc3ed6b4c6f860f97165ac2f7bb6f2e2cb192a9abd49795be5bcf37d8ee69a6e169c24e5c32e4e7fa33265461407f952ba49e204818a2f785f113f922b8b0240253f9470390d39049303777ddbcb9750e9d64849ce0903eae704dc9f589b7680deb9d609fd5bcd4decdd6f120542e5cfff5d76f2a43c8615fb5b3a9213463797aa9024100a1ddf023c0cd94c019bb26d09b9e3ca8fa971cb16aa58b9baf79d6081a1dbba452ba53653e2804ba98ff69e8bb1b3a161ea225ea501463216a8dab9b88a75e5f02406178646e112cf79d921a8a843f17f6e7ff974f688122365bf6690cdfc996e1890952eb3820dd1890ec1c8619e87a2bd38f9d03b37fac742efb748c7885942c39"/>
0024	</KeyValue>
0025	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0026	<CryptographicLength type="Integer" value="1024"/>
0027	</KeyBlock>
0028	</PrivateKey>
0029	</RequestPayload>
0030	</BatchItem>
0031	</RequestMessage>
0032	<ResponseMessage>
0033	<ResponseHeader>
0034	<ProtocolVersion>
0035	<ProtocolVersionMajor type="Integer" value="1"/>
0036	<ProtocolVersionMinor type="Integer" value="0"/>
0037	</ProtocolVersion>
0038	<TimeStamp type="DateTime" value="2010-02-11T08:49:37+00:00"/>
0039	<BatchCount type="Integer" value="1"/>
0040	</ResponseHeader>
0041	<BatchItem>
0042	<Operation type="Enumeration" value="Register"/>
0043	<ResultStatus type="Enumeration" value="Success"/>
0044	<ResponsePayload>
0045	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0046	</ResponsePayload>
0047	</BatchItem>
0048	</ResponseMessage>
	# TIME 1
0049	<RequestMessage>
0050	<RequestHeader>
0051	<ProtocolVersion>
0052	<ProtocolVersionMajor type="Integer" value="1"/>
0053	<ProtocolVersionMinor type="Integer" value="0"/>
0054	</ProtocolVersion>
0055	<BatchCount type="Integer" value="1"/>
0056	</RequestHeader>
0057	<BatchItem>
0058	<Operation type="Enumeration" value="Register"/>
0059	<RequestPayload>
0060	<ObjectType type="Enumeration" value="PublicKey"/>
0061	<TemplateAttribute>
0062	<Attribute>
0063	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0064	<AttributeValue type="Integer" value="Verify"/>

0065	</Attribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Link"/>
0068	<AttributeValue>
0069	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0070	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0071	</AttributeValue>
0072	</Attribute>
0073	</TemplateAttribute>
0074	<PublicKey>
0075	<KeyBlock>
0076	<KeyFormatType type="Enumeration" value="X_509"/>
0077	<KeyValue>
0078	<KeyMaterial type="ByteString"
	value="30819f300d06092a864886f70d010101050003818d0030818902818100930
	451c9ecd94f5bb9da17dd09381bd23be43eca8c7539f301fc8a8cd5d5274c3e7699d
	bdc711c97a7aa91e2c50a82bd0b1034f0df493dec16362427e58acce7f6ce0f9bcc6
	17bbd8c90d0094a2703ba0d09eb19d1005f2fb265526aac75af32f8bc782cded2a57
	f811e03eaf67a944de5e78413dca8f232d074e6dcea4cec9f0203010001"/>
0079	</KeyValue>
0080	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0081	<CryptographicLength type="Integer" value="1024"/>
0082	</KeyBlock>
0083	</PublicKey>
0084	</RequestPayload>
0085	</BatchItem>
0086	</RequestMessage>
0087	<ResponseMessage>
0088	<ResponseHeader>
0089	<ProtocolVersion>
0090	<ProtocolVersionMajor type="Integer" value="1"/>
0091	<ProtocolVersionMinor type="Integer" value="0"/>
0092	</ProtocolVersion>
0093	<TimeStamp type="DateTime" value="2010-02-11T08:49:38+00:00"/>
0094	<BatchCount type="Integer" value="1"/>
0095	</ResponseHeader>
0096	<BatchItem>
0097	<Operation type="Enumeration" value="Register"/>
0098	<ResultStatus type="Enumeration" value="Success"/>
0099	<ResponsePayload>
0100	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0101	</ResponsePayload>
0102	</BatchItem>
0103	</ResponseMessage>
	# TIME 2
0104	<RequestMessage>
0105	<RequestHeader>
0106	<ProtocolVersion>
0107	<ProtocolVersionMajor type="Integer" value="1"/>
0108	<ProtocolVersionMinor type="Integer" value="0"/>
0109	</ProtocolVersion>
0110	<BatchCount type="Integer" value="1"/>
0111	</RequestHeader>
0112	<BatchItem>
0113	<Operation type="Enumeration" value="AddAttribute"/>

0114	<RequestPayload>
0115	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0116	<Attribute>
0117	<AttributeName type="TextString" value="Link"/>
0118	<AttributeValue>
0119	<LinkType type="Enumeration" value="PublicKeyLink"/>
0120	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0121	</AttributeValue>
0122	</Attribute>
0123	</RequestPayload>
0124	</BatchItem>
0125	</RequestMessage>
0126	<ResponseMessage>
0127	<ResponseHeader>
0128	<ProtocolVersion>
0129	<ProtocolVersionMajor type="Integer" value="1"/>
0130	<ProtocolVersionMinor type="Integer" value="0"/>
0131	</ProtocolVersion>
0132	<TimeStamp type="DateTime" value="2010-02-11T08:49:38+00:00"/>
0133	<BatchCount type="Integer" value="1"/>
0134	</ResponseHeader>
0135	<BatchItem>
0136	<Operation type="Enumeration" value="AddAttribute"/>
0137	<ResultStatus type="Enumeration" value="Success"/>
0138	<ResponsePayload>
0139	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0140	<Attribute>
0141	<AttributeName type="TextString" value="Link"/>
0142	<AttributeValue>
0143	<LinkType type="Enumeration" value="PublicKeyLink"/>
0144	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0145	</AttributeValue>
0146	</Attribute>
0147	</ResponsePayload>
0148	</BatchItem>
0149	</ResponseMessage>
	# TIME 3
0150	<RequestMessage>
0151	<RequestHeader>
0152	<ProtocolVersion>
0153	<ProtocolVersionMajor type="Integer" value="1"/>
0154	<ProtocolVersionMinor type="Integer" value="0"/>
0155	</ProtocolVersion>
0156	<BatchCount type="Integer" value="1"/>
0157	</RequestHeader>
0158	<BatchItem>
0159	<Operation type="Enumeration" value="Locate"/>
0160	<RequestPayload>
0161	<Attribute>
0162	<AttributeName type="TextString" value="Object Type"/>
0163	<AttributeValue type="Enumeration" value="PublicKey"/>
0164	</Attribute>
0165	<Attribute>

0166	<AttributeName type="TextString" value="Link"/>
0167	<AttributeValue>
0168	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0169	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0170	</AttributeValue>
0171	</Attribute>
0172	</RequestPayload>
0173	</BatchItem>
0174	</RequestMessage>
0175	<ResponseMessage>
0176	<ResponseHeader>
0177	<ProtocolVersion>
0178	<ProtocolVersionMajor type="Integer" value="1"/>
0179	<ProtocolVersionMinor type="Integer" value="0"/>
0180	</ProtocolVersion>
0181	<TimeStamp type="DateTime" value="2010-02-11T08:49:38+00:00"/>
0182	<BatchCount type="Integer" value="1"/>
0183	</ResponseHeader>
0184	<BatchItem>
0185	<Operation type="Enumeration" value="Locate"/>
0186	<ResultStatus type="Enumeration" value="Success"/>
0187	<ResponsePayload>
0188	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0189	</ResponsePayload>
0190	</BatchItem>
0191	</ResponseMessage>
	# TIME 4
0192	<RequestMessage>
0193	<RequestHeader>
0194	<ProtocolVersion>
0195	<ProtocolVersionMajor type="Integer" value="1"/>
0196	<ProtocolVersionMinor type="Integer" value="0"/>
0197	</ProtocolVersion>
0198	<BatchCount type="Integer" value="1"/>
0199	</RequestHeader>
0200	<BatchItem>
0201	<Operation type="Enumeration" value="Locate"/>
0202	<RequestPayload>
0203	<Attribute>
0204	<AttributeName type="TextString" value="Object Type"/>
0205	<AttributeValue type="Enumeration" value="PrivateKey"/>
0206	</Attribute>
0207	<Attribute>
0208	<AttributeName type="TextString" value="Link"/>
0209	<AttributeValue>
0210	<LinkType type="Enumeration" value="PublicKeyLink"/>
0211	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0212	</AttributeValue>
0213	</Attribute>
0214	</RequestPayload>
0215	</BatchItem>
0216	</RequestMessage>
0217	<ResponseMessage>

0218	<ResponseHeader>
0219	<ProtocolVersion>
0220	<ProtocolVersionMajor type="Integer" value="1"/>
0221	<ProtocolVersionMinor type="Integer" value="0"/>
0222	</ProtocolVersion>
0223	<TimeStamp type="DateTime" value="2010-02-11T08:49:39+00:00"/>
0224	<BatchCount type="Integer" value="1"/>
0225	</ResponseHeader>
0226	<BatchItem>
0227	<Operation type="Enumeration" value="Locate"/>
0228	<ResultStatus type="Enumeration" value="Success"/>
0229	<ResponsePayload>
0230	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0231	</ResponsePayload>
0232	</BatchItem>
0233	</ResponseMessage>
# TIME 5	
0234	<RequestMessage>
0235	<RequestHeader>
0236	<ProtocolVersion>
0237	<ProtocolVersionMajor type="Integer" value="1"/>
0238	<ProtocolVersionMinor type="Integer" value="0"/>
0239	</ProtocolVersion>
0240	<BatchCount type="Integer" value="1"/>
0241	</RequestHeader>
0242	<BatchItem>
0243	<Operation type="Enumeration" value="Destroy"/>
0244	<RequestPayload>
0245	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0246	</RequestPayload>
0247	</BatchItem>
0248	</RequestMessage>
0249	<ResponseMessage>
0250	<ResponseHeader>
0251	<ProtocolVersion>
0252	<ProtocolVersionMajor type="Integer" value="1"/>
0253	<ProtocolVersionMinor type="Integer" value="0"/>
0254	</ProtocolVersion>
0255	<TimeStamp type="DateTime" value="2010-02-11T08:49:39+00:00"/>
0256	<BatchCount type="Integer" value="1"/>
0257	</ResponseHeader>
0258	<BatchItem>
0259	<Operation type="Enumeration" value="Destroy"/>
0260	<ResultStatus type="Enumeration" value="Success"/>
0261	<ResponsePayload>
0262	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0263	</ResponsePayload>
0264	</BatchItem>
0265	</ResponseMessage>
# TIME 6	
0266	<RequestMessage>
0267	<RequestHeader>
0268	<ProtocolVersion>

0269	<ProtocolVersionMajor type="Integer" value="1"/>
0270	<ProtocolVersionMinor type="Integer" value="0"/>
0271	</ProtocolVersion>
0272	<BatchCount type="Integer" value="1"/>
0273	</RequestHeader>
0274	<BatchItem>
0275	<Operation type="Enumeration" value="Destroy"/>
0276	<RequestPayload>
0277	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0278	</RequestPayload>
0279	</BatchItem>
0280	</RequestMessage>
0281	<ResponseMessage>
0282	<ResponseHeader>
0283	<ProtocolVersion>
0284	<ProtocolVersionMajor type="Integer" value="1"/>
0285	<ProtocolVersionMinor type="Integer" value="0"/>
0286	</ProtocolVersion>
0287	<TimeStamp type="DateTime" value="2010-02-11T08:49:39+00:00"/>
0288	<BatchCount type="Integer" value="1"/>
0289	</ResponseHeader>
0290	<BatchItem>
0291	<Operation type="Enumeration" value="Destroy"/>
0292	<ResultStatus type="Enumeration" value="Success"/>
0293	<ResponsePayload>
0294	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0295	</ResponsePayload>
0296	</BatchItem>
0297	</ResponseMessage>

136

137 2.1.14 TC-91-10 - Create a Key, Re-key

138 Create a symmetric key with a specific name, and then use Locate to find the key. After using
139 Re-key to create a new key, verify that the name was removed from the existing key and copied
140 to the new key. Also verify that the key material for the old key is still retrievable. To clean up,
141 both keys are deleted.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>

0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
0020	Length"/>
0021	<AttributeValue type="Integer" value="128"/>
0022	</Attribute>
0023	<AttributeName type="TextString" value="Cryptographic
0024	Usage Mask"/>
0025	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0026	</Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="rekeyKey"/>
0030	<NameType type="Enumeration"
0031	value="UninterpretedTextString"/>
0032	</AttributeValue>
0033	</Attribute>
0034	</TemplateAttribute>
0035	</RequestPayload>
0036	</BatchItem>
0037	</RequestMessage>
0038	<ResponseMessage>
0039	<ResponseHeader>
0040	<ProtocolVersion>
0041	<ProtocolVersionMajor type="Integer" value="1"/>
0042	<ProtocolVersionMinor type="Integer" value="0"/>
0043	</ProtocolVersion>
0044	<TimeStamp type="DateTime" value="2010-02-11T09:07:06+00:00"/>
0045	<BatchCount type="Integer" value="1"/>
0046	</ResponseHeader>
0047	<BatchItem>
0048	<Operation type="Enumeration" value="Create"/>
0049	<ResultStatus type="Enumeration" value="Success"/>
0050	<ResponsePayload>
0051	<ObjectType type="Enumeration" value="SymmetricKey"/>
0052	<UniqueIdentifier type="TextString"
0053	value="\$UNIQUE_IDENTIFIER_0"/>
0054	</ResponsePayload>
0055	</BatchItem>
0056	</ResponseMessage>
0057	# TIME 1
0058	<RequestMessage>
0059	<RequestHeader>
0060	<ProtocolVersion>
0061	<ProtocolVersionMajor type="Integer" value="1"/>
0062	<ProtocolVersionMinor type="Integer" value="0"/>
0063	</ProtocolVersion>
0064	<BatchCount type="Integer" value="1"/>
0065	</RequestHeader>
	<BatchItem>
	<Operation type="Enumeration" value="Locate"/>
	<RequestPayload>

0066	<Attribute>
0067	<AttributeName type="TextString" value="Name"/>
0068	<AttributeValue>
0069	<NameValue type="TextString" value="rekeyKey"/>
0070	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0071	</AttributeValue>
0072	</Attribute>
0073	</RequestPayload>
0074	</BatchItem>
0075	</RequestMessage>
0076	<ResponseMessage>
0077	<ResponseHeader>
0078	<ProtocolVersion>
0079	<ProtocolVersionMajor type="Integer" value="1"/>
0080	<ProtocolVersionMinor type="Integer" value="0"/>
0081	</ProtocolVersion>
0082	<TimeStamp type="DateTime" value="2010-02-11T09:07:06+00:00"/>
0083	<BatchCount type="Integer" value="1"/>
0084	</ResponseHeader>
0085	<BatchItem>
0086	<Operation type="Enumeration" value="Locate"/>
0087	<ResultStatus type="Enumeration" value="Success"/>
0088	<ResponsePayload>
0089	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0090	</ResponsePayload>
0091	</BatchItem>
0092	</ResponseMessage>
0093	# TIME 2
0093	<RequestMessage>
0094	<RequestHeader>
0095	<ProtocolVersion>
0096	<ProtocolVersionMajor type="Integer" value="1"/>
0097	<ProtocolVersionMinor type="Integer" value="0"/>
0098	</ProtocolVersion>
0099	<BatchCount type="Integer" value="1"/>
0100	</RequestHeader>
0101	<BatchItem>
0102	<Operation type="Enumeration" value="ReKey"/>
0103	<RequestPayload>
0104	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0105	</RequestPayload>
0106	</BatchItem>
0107	</RequestMessage>
0108	<ResponseMessage>
0109	<ResponseHeader>
0110	<ProtocolVersion>
0111	<ProtocolVersionMajor type="Integer" value="1"/>
0112	<ProtocolVersionMinor type="Integer" value="0"/>
0113	</ProtocolVersion>
0114	<TimeStamp type="DateTime" value="2010-02-11T09:07:07+00:00"/>
0115	<BatchCount type="Integer" value="1"/>
0116	</ResponseHeader>
0117	<BatchItem>

0118	<Operation type="Enumeration" value="ReKey"/>
0119	<ResultStatus type="Enumeration" value="Success"/>
0120	<ResponsePayload>
0121	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0122	</ResponsePayload>
0123	</BatchItem>
0124	</ResponseMessage>
	# TIME 3
0125	<RequestMessage>
0126	<RequestHeader>
0127	<ProtocolVersion>
0128	<ProtocolVersionMajor type="Integer" value="1"/>
0129	<ProtocolVersionMinor type="Integer" value="0"/>
0130	</ProtocolVersion>
0131	<BatchCount type="Integer" value="1"/>
0132	</RequestHeader>
0133	<BatchItem>
0134	<Operation type="Enumeration" value="Locate"/>
0135	<RequestPayload>
0136	<Attribute>
0137	<AttributeName type="TextString" value="Name"/>
0138	<AttributeValue>
0139	<NameValue type="TextString" value="rekeyKey"/>
0140	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0141	</AttributeValue>
0142	</Attribute>
0143	</RequestPayload>
0144	</BatchItem>
0145	</RequestMessage>
0146	<ResponseMessage>
0147	<ResponseHeader>
0148	<ProtocolVersion>
0149	<ProtocolVersionMajor type="Integer" value="1"/>
0150	<ProtocolVersionMinor type="Integer" value="0"/>
0151	</ProtocolVersion>
0152	<TimeStamp type="DateTime" value="2010-02-11T09:07:07+00:00"/>
0153	<BatchCount type="Integer" value="1"/>
0154	</ResponseHeader>
0155	<BatchItem>
0156	<Operation type="Enumeration" value="Locate"/>
0157	<ResultStatus type="Enumeration" value="Success"/>
0158	<ResponsePayload>
0159	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0160	</ResponsePayload>
0161	</BatchItem>
0162	</ResponseMessage>
	# TIME 4
0163	<RequestMessage>
0164	<RequestHeader>
0165	<ProtocolVersion>
0166	<ProtocolVersionMajor type="Integer" value="1"/>
0167	<ProtocolVersionMinor type="Integer" value="0"/>
0168	</ProtocolVersion>

0169	<BatchCount type="Integer" value="1"/>
0170	</RequestHeader>
0171	<BatchItem>
0172	<Operation type="Enumeration" value="GetAttributes"/>
0173	<RequestPayload>
0174	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0175	<AttributeName type="TextString" value="Name"/>
0176	</RequestPayload>
0177	</BatchItem>
0178	</RequestMessage>
0179	<ResponseMessage>
0180	<ResponseHeader>
0181	<ProtocolVersion>
0182	<ProtocolVersionMajor type="Integer" value="1"/>
0183	<ProtocolVersionMinor type="Integer" value="0"/>
0184	</ProtocolVersion>
0185	<TimeStamp type="DateTime" value="2010-02-11T09:07:07+00:00"/>
0186	<BatchCount type="Integer" value="1"/>
0187	</ResponseHeader>
0188	<BatchItem>
0189	<Operation type="Enumeration" value="GetAttributes"/>
0190	<ResultStatus type="Enumeration" value="Success"/>
0191	<ResponsePayload>
0192	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0193	</ResponsePayload>
0194	</BatchItem>
0195	</ResponseMessage>
	# TIME 5
0196	<RequestMessage>
0197	<RequestHeader>
0198	<ProtocolVersion>
0199	<ProtocolVersionMajor type="Integer" value="1"/>
0200	<ProtocolVersionMinor type="Integer" value="0"/>
0201	</ProtocolVersion>
0202	<BatchCount type="Integer" value="1"/>
0203	</RequestHeader>
0204	<BatchItem>
0205	<Operation type="Enumeration" value="Get"/>
0206	<RequestPayload>
0207	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0208	</RequestPayload>
0209	</BatchItem>
0210	</RequestMessage>
0211	<ResponseMessage>
0212	<ResponseHeader>
0213	<ProtocolVersion>
0214	<ProtocolVersionMajor type="Integer" value="1"/>
0215	<ProtocolVersionMinor type="Integer" value="0"/>
0216	</ProtocolVersion>
0217	<TimeStamp type="DateTime" value="2010-02-11T09:07:07+00:00"/>
0218	<BatchCount type="Integer" value="1"/>
0219	</ResponseHeader>
0220	<BatchItem>

0221	<Operation type="Enumeration" value="Get"/>
0222	<ResultStatus type="Enumeration" value="Success"/>
0223	<ResponsePayload>
0224	<ObjectType type="Enumeration" value="SymmetricKey"/>
0225	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0226	<SymmetricKey>
0227	<KeyBlock>
0228	<KeyFormatType type="Enumeration" value="Raw"/>
0229	<KeyValue>
0230	<KeyMaterial type="ByteString"
	value="bc25617991c49d06536008d076017462"/>
0231	</KeyValue>
0232	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0233	<CryptographicLength type="Integer" value="128"/>
0234	</KeyBlock>
0235	</SymmetricKey>
0236	</ResponsePayload>
0237	</BatchItem>
0238	</ResponseMessage>
	# TIME 6
0239	<RequestMessage>
0240	<RequestHeader>
0241	<ProtocolVersion>
0242	<ProtocolVersionMajor type="Integer" value="1"/>
0243	<ProtocolVersionMinor type="Integer" value="0"/>
0244	</ProtocolVersion>
0245	<BatchCount type="Integer" value="1"/>
0246	</RequestHeader>
0247	<BatchItem>
0248	<Operation type="Enumeration" value="Destroy"/>
0249	<RequestPayload>
0250	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0251	</RequestPayload>
0252	</BatchItem>
0253	</RequestMessage>
0254	<ResponseMessage>
0255	<ResponseHeader>
0256	<ProtocolVersion>
0257	<ProtocolVersionMajor type="Integer" value="1"/>
0258	<ProtocolVersionMinor type="Integer" value="0"/>
0259	</ProtocolVersion>
0260	<TimeStamp type="DateTime" value="2010-02-11T09:07:08+00:00"/>
0261	<BatchCount type="Integer" value="1"/>
0262	</ResponseHeader>
0263	<BatchItem>
0264	<Operation type="Enumeration" value="Destroy"/>
0265	<ResultStatus type="Enumeration" value="Success"/>
0266	<ResponsePayload>
0267	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0268	</ResponsePayload>
0269	</BatchItem>
0270	</ResponseMessage>
	# TIME 7

0271	<RequestMessage>
0272	<RequestHeader>
0273	<ProtocolVersion>
0274	<ProtocolVersionMajor type="Integer" value="1"/>
0275	<ProtocolVersionMinor type="Integer" value="0"/>
0276	</ProtocolVersion>
0277	<BatchCount type="Integer" value="1"/>
0278	</RequestHeader>
0279	<BatchItem>
0280	<Operation type="Enumeration" value="Destroy"/>
0281	<RequestPayload>
0282	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0283	</RequestPayload>
0284	</BatchItem>
0285	</RequestMessage>
0286	<ResponseMessage>
0287	<ResponseHeader>
0288	<ProtocolVersion>
0289	<ProtocolVersionMajor type="Integer" value="1"/>
0290	<ProtocolVersionMinor type="Integer" value="0"/>
0291	</ProtocolVersion>
0292	<TimeStamp type="DateTime" value="2010-02-11T09:07:08+00:00"/>
0293	<BatchCount type="Integer" value="1"/>
0294	</ResponseHeader>
0295	<BatchItem>
0296	<Operation type="Enumeration" value="Destroy"/>
0297	<ResultStatus type="Enumeration" value="Success"/>
0298	<ResponsePayload>
0299	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0300	</ResponsePayload>
0301	</BatchItem>
0302	</ResponseMessage>

142

143 2.1.15 TC-92-10 - Existing Key Expired, Re-key with Same Life-cycle

144 Create a new symmetric key. Then add the Activation Date and Deactivation Date attributes
145 based on the timestamp in the response to the Create request. The Activation Date is set to the
146 current time and the Deactivation Date to a time in the near future. Repeated Get Attribute calls
147 are performed to verify that the state is first 'Active', then subsequently 'Deactivated'. Then
148 issue a Re-key request, including an Offset value of zero leading to the Activation Date of the
149 replacement key to be set to the same value as the Initial Date of the replacement key. Verify
150 from the response that the Activation Date and Deactivation Date attributes were set correctly
151 (if they are not returned, issue a Get Attribute request). Do a Get Attribute operation to verify
152 that the state of the new key is 'Active'. To clean up, both keys are deleted.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>

0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="rekeyKey"/>
0030	<NameType type="Enumeration" value="UninterpretedTextString"/>
0031	</AttributeValue>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="0"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2010-02-11T13:01:59+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
	# TIME 1
0055	<RequestMessage>
0056	<RequestHeader>

0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="0"/>
0060	</ProtocolVersion>
0061	<BatchOrderOption type="Boolean" value="true"/>
0062	<BatchCount type="Integer" value="2"/>
0063	</RequestHeader>
0064	<BatchItem>
0065	<Operation type="Enumeration" value="AddAttribute"/>
0066	<UniqueBatchItemID type="ByteString" value="bac4a9cecc650259"/>
0067	<RequestPayload>
0068	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0069	<Attribute>
0070	<AttributeName type="TextString" value="Activation Date"/>
0071	<AttributeValue type="DateTime" value="2009-02-
	11T13:01:59+00:00"/>
0072	</Attribute>
0073	</RequestPayload>
0074	</BatchItem>
0075	<BatchItem>
0076	<Operation type="Enumeration" value="AddAttribute"/>
0077	<UniqueBatchItemID type="ByteString" value="582c952324f4552f"/>
0078	<RequestPayload>
0079	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0080	<Attribute>
0081	<AttributeName type="TextString" value="Deactivation Date"/>
0082	<AttributeValue type="DateTime" value="2010-02-
	11T13:03:59+00:00"/>
0083	</Attribute>
0084	</RequestPayload>
0085	</BatchItem>
0086	</RequestMessage>
0087	<ResponseMessage>
0088	<ResponseHeader>
0089	<ProtocolVersion>
0090	<ProtocolVersionMajor type="Integer" value="1"/>
0091	<ProtocolVersionMinor type="Integer" value="0"/>
0092	</ProtocolVersion>
0093	<TimeStamp type="DateTime" value="2010-02-11T13:01:59+00:00"/>
0094	<BatchCount type="Integer" value="2"/>
0095	</ResponseHeader>
0096	<BatchItem>
0097	<Operation type="Enumeration" value="AddAttribute"/>
0098	<UniqueBatchItemID type="ByteString" value="bac4a9cecc650259"/>
0099	<ResultStatus type="Enumeration" value="Success"/>
0100	<ResponsePayload>
0101	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0102	<Attribute>
0103	<AttributeName type="TextString" value="Activation Date"/>
0104	<AttributeValue type="DateTime" value="2009-02-
	11T13:01:59+00:00"/>
0105	</Attribute>
0106	</ResponsePayload>
0107	</BatchItem>

0108	<BatchItem>
0109	<Operation type="Enumeration" value="AddAttribute"/>
0110	<UniqueBatchItemID type="ByteString" value="582c952324f4552f"/>
0111	<ResultStatus type="Enumeration" value="Success"/>
0112	<ResponsePayload>
0113	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0114	<Attribute>
0115	<AttributeName type="TextString" value="Deactivation Date"/>
0116	<AttributeValue type="DateTime" value="2010-02-
	11T13:03:59+00:00"/>
0117	</Attribute>
0118	</ResponsePayload>
0119	</BatchItem>
0120	</ResponseMessage>
	# TIME 2
0121	<RequestMessage>
0122	<RequestHeader>
0123	<ProtocolVersion>
0124	<ProtocolVersionMajor type="Integer" value="1"/>
0125	<ProtocolVersionMinor type="Integer" value="0"/>
0126	</ProtocolVersion>
0127	<BatchCount type="Integer" value="1"/>
0128	</RequestHeader>
0129	<BatchItem>
0130	<Operation type="Enumeration" value="GetAttributes"/>
0131	<RequestPayload>
0132	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0133	<AttributeName type="TextString" value="State"/>
0134	</RequestPayload>
0135	</BatchItem>
0136	</RequestMessage>
0137	<ResponseMessage>
0138	<ResponseHeader>
0139	<ProtocolVersion>
0140	<ProtocolVersionMajor type="Integer" value="1"/>
0141	<ProtocolVersionMinor type="Integer" value="0"/>
0142	</ProtocolVersion>
0143	<TimeStamp type="DateTime" value="2010-02-11T13:01:59+00:00"/>
0144	<BatchCount type="Integer" value="1"/>
0145	</ResponseHeader>
0146	<BatchItem>
0147	<Operation type="Enumeration" value="GetAttributes"/>
0148	<ResultStatus type="Enumeration" value="Success"/>
0149	<ResponsePayload>
0150	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0151	<Attribute>
0152	<AttributeName type="TextString" value="State"/>
0153	<AttributeValue type="Enumeration" value="Active"/>
0154	</Attribute>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
	# TIME 3

0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="0"/>
0163	</ProtocolVersion>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="GetAttributes"/>
0168	<RequestPayload>
0169	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0170	<AttributeName type="TextString" value="State"/>
0171	</RequestPayload>
0172	</BatchItem>
0173	</RequestMessage>
0174	<ResponseMessage>
0175	<ResponseHeader>
0176	<ProtocolVersion>
0177	<ProtocolVersionMajor type="Integer" value="1"/>
0178	<ProtocolVersionMinor type="Integer" value="0"/>
0179	</ProtocolVersion>
0180	<TimeStamp type="DateTime" value="2010-02-11T13:04:00+00:00"/>
0181	<BatchCount type="Integer" value="1"/>
0182	</ResponseHeader>
0183	<BatchItem>
0184	<Operation type="Enumeration" value="GetAttributes"/>
0185	<ResultStatus type="Enumeration" value="Success"/>
0186	<ResponsePayload>
0187	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0188	<Attribute>
0189	<AttributeName type="TextString" value="State"/>
0190	<AttributeValue type="Enumeration" value="Deactivated"/>
0191	</Attribute>
0192	</ResponsePayload>
0193	</BatchItem>
0194	</ResponseMessage>
	# TIME 4
0195	<RequestMessage>
0196	<RequestHeader>
0197	<ProtocolVersion>
0198	<ProtocolVersionMajor type="Integer" value="1"/>
0199	<ProtocolVersionMinor type="Integer" value="0"/>
0200	</ProtocolVersion>
0201	<BatchCount type="Integer" value="1"/>
0202	</RequestHeader>
0203	<BatchItem>
0204	<Operation type="Enumeration" value="ReKey"/>
0205	<RequestPayload>
0206	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0207	<Offset type="Interval" value="0"/>
0208	</RequestPayload>
0209	</BatchItem>
0210	</RequestMessage>

0211	<ResponseMessage>
0212	<ResponseHeader>
0213	<ProtocolVersion>
0214	<ProtocolVersionMajor type="Integer" value="1"/>
0215	<ProtocolVersionMinor type="Integer" value="0"/>
0216	</ProtocolVersion>
0217	<TimeStamp type="DateTime" value="2010-02-11T13:04:00+00:00"/>
0218	<BatchCount type="Integer" value="1"/>
0219	</ResponseHeader>
0220	<BatchItem>
0221	<Operation type="Enumeration" value="ReKey"/>
0222	<ResultStatus type="Enumeration" value="Success"/>
0223	<ResponsePayload>
0224	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0225	</ResponsePayload>
0226	</BatchItem>
0227	</ResponseMessage>
# TIME 5	
0228	<RequestMessage>
0229	<RequestHeader>
0230	<ProtocolVersion>
0231	<ProtocolVersionMajor type="Integer" value="1"/>
0232	<ProtocolVersionMinor type="Integer" value="0"/>
0233	</ProtocolVersion>
0234	<BatchCount type="Integer" value="1"/>
0235	</RequestHeader>
0236	<BatchItem>
0237	<Operation type="Enumeration" value="GetAttributes"/>
0238	<RequestPayload>
0239	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0240	<AttributeName type="TextString" value="Activation Date"/>
0241	<AttributeName type="TextString" value="Deactivation Date"/>
0242	</RequestPayload>
0243	</BatchItem>
0244	</RequestMessage>
0245	<ResponseMessage>
0246	<ResponseHeader>
0247	<ProtocolVersion>
0248	<ProtocolVersionMajor type="Integer" value="1"/>
0249	<ProtocolVersionMinor type="Integer" value="0"/>
0250	</ProtocolVersion>
0251	<TimeStamp type="DateTime" value="2010-02-11T13:04:00+00:00"/>
0252	<BatchCount type="Integer" value="1"/>
0253	</ResponseHeader>
0254	<BatchItem>
0255	<Operation type="Enumeration" value="GetAttributes"/>
0256	<ResultStatus type="Enumeration" value="Success"/>
0257	<ResponsePayload>
0258	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0259	<Attribute>
0260	<AttributeName type="TextString" value="Activation Date"/>
0261	<AttributeValue type="DateTime" value="2009-04-
	17T13:01:58+00:00"/>
0262	</Attribute>

0263	<Attribute>
0264	<AttributeName type="TextString" value="Deactivation Date"/>
0265	<AttributeValue type="DateTime" value="2010-04-17T13:03:58+00:00"/>
0266	</Attribute>
0267	</ResponsePayload>
0268	</BatchItem>
0269	</ResponseMessage>
# TIME 6	
0270	<RequestMessage>
0271	<RequestHeader>
0272	<ProtocolVersion>
0273	<ProtocolVersionMajor type="Integer" value="1"/>
0274	<ProtocolVersionMinor type="Integer" value="0"/>
0275	</ProtocolVersion>
0276	<BatchCount type="Integer" value="1"/>
0277	</RequestHeader>
0278	<BatchItem>
0279	<Operation type="Enumeration" value="GetAttributes"/>
0280	<RequestPayload>
0281	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0282	<AttributeName type="TextString" value="State"/>
0283	</RequestPayload>
0284	</BatchItem>
0285	</RequestMessage>
0286	<ResponseMessage>
0287	<ResponseHeader>
0288	<ProtocolVersion>
0289	<ProtocolVersionMajor type="Integer" value="1"/>
0290	<ProtocolVersionMinor type="Integer" value="0"/>
0291	</ProtocolVersion>
0292	<TimeStamp type="DateTime" value="2010-02-11T13:04:00+00:00"/>
0293	<BatchCount type="Integer" value="1"/>
0294	</ResponseHeader>
0295	<BatchItem>
0296	<Operation type="Enumeration" value="GetAttributes"/>
0297	<ResultStatus type="Enumeration" value="Success"/>
0298	<ResponsePayload>
0299	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0300	<Attribute>
0301	<AttributeName type="TextString" value="State"/>
0302	<AttributeValue type="Enumeration" value="Active"/>
0303	</Attribute>
0304	</ResponsePayload>
0305	</BatchItem>
0306	</ResponseMessage>
# TIME 7	
0307	<RequestMessage>
0308	<RequestHeader>
0309	<ProtocolVersion>
0310	<ProtocolVersionMajor type="Integer" value="1"/>
0311	<ProtocolVersionMinor type="Integer" value="0"/>
0312	</ProtocolVersion>
0313	<BatchCount type="Integer" value="1"/>

0314	</RequestHeader>
0315	<BatchItem>
0316	<Operation type="Enumeration" value="Destroy"/>
0317	<RequestPayload>
0318	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0319	</RequestPayload>
0320	</BatchItem>
0321	</RequestMessage>
0322	<ResponseMessage>
0323	<ResponseHeader>
0324	<ProtocolVersion>
0325	<ProtocolVersionMajor type="Integer" value="1"/>
0326	<ProtocolVersionMinor type="Integer" value="0"/>
0327	</ProtocolVersion>
0328	<TimeStamp type="DateTime" value="2010-02-11T13:04:00+00:00"/>
0329	<BatchCount type="Integer" value="1"/>
0330	</ResponseHeader>
0331	<BatchItem>
0332	<Operation type="Enumeration" value="Destroy"/>
0333	<ResultStatus type="Enumeration" value="Success"/>
0334	<ResponsePayload>
0335	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0336	</ResponsePayload>
0337	</BatchItem>
0338	</ResponseMessage>
	# TIME 8
0339	<RequestMessage>
0340	<RequestHeader>
0341	<ProtocolVersion>
0342	<ProtocolVersionMajor type="Integer" value="1"/>
0343	<ProtocolVersionMinor type="Integer" value="0"/>
0344	</ProtocolVersion>
0345	<BatchOrderOption type="Boolean" value="true"/>
0346	<BatchCount type="Integer" value="2"/>
0347	</RequestHeader>
0348	<BatchItem>
0349	<Operation type="Enumeration" value="Revoke"/>
0350	<UniqueBatchItemID type="ByteString" value="7012417aa1b7394b"/>
0351	<RequestPayload>
0352	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0353	<RevocationReason>
0354	<RevocationReasonCode type="Enumeration"
	value="CessationOfOperation"/>
0355	</RevocationReason>
0356	</RequestPayload>
0357	</BatchItem>
0358	<BatchItem>
0359	<Operation type="Enumeration" value="Destroy"/>
0360	<UniqueBatchItemID type="ByteString" value="3f8f4f1759704555"/>
0361	<RequestPayload>
0362	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0363	</RequestPayload>
0364	</BatchItem>

0365	</RequestMessage>
0366	<ResponseMessage>
0367	<ResponseHeader>
0368	<ProtocolVersion>
0369	<ProtocolVersionMajor type="Integer" value="1"/>
0370	<ProtocolVersionMinor type="Integer" value="0"/>
0371	</ProtocolVersion>
0372	<TimeStamp type="DateTime" value="2010-02-11T13:04:00+00:00"/>
0373	<BatchCount type="Integer" value="2"/>
0374	</ResponseHeader>
0375	<BatchItem>
0376	<Operation type="Enumeration" value="Revoke"/>
0377	<UniqueBatchItemID type="ByteString" value="7012417aa1b7394b"/>
0378	<ResultStatus type="Enumeration" value="Success"/>
0379	<ResponsePayload>
0380	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0381	</ResponsePayload>
0382	</BatchItem>
0383	<BatchItem>
0384	<Operation type="Enumeration" value="Destroy"/>
0385	<UniqueBatchItemID type="ByteString" value="3f8f4f1759704555"/>
0386	<ResultStatus type="Enumeration" value="Success"/>
0387	<ResponsePayload>
0388	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0389	</ResponsePayload>
0390	</BatchItem>
0391	</ResponseMessage>

153

154 2.1.16 TC-93-10 - Existing Key Compromised, Re-key with Same Life-cycle

155 Create a new symmetric key with the Activation Date in the past. Do a Get Attribute operation
156 on the State attribute to verify the key is 'Active'. Then revoke the key as compromised, verify
157 that the state has changed to 'Compromised'. Create a replacement key using Re-key with the
158 offset set to '0' to indicate that the times are to be copied from the existing key. Do a Get
159 Attribute operation to verify that the state of the new key is 'Active'. To clean up, both keys are
160 deleted.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>

0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
0020	Length"/>
0021	<AttributeValue type="Integer" value="128"/>
0022	</Attribute>
0023	<AttributeName type="TextString" value="Cryptographic
0024	Usage Mask"/>
0025	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0026	</Attribute>
0027	<AttributeName type="TextString" value="Activation Date"/>
0028	<AttributeValue type="DateTime" value="2010-02-
0029	11T14:12:23+00:00"/>
0030	</Attribute>
0031	<AttributeName type="TextString" value="Name"/>
0032	<AttributeValue>
0033	<NameValue type="TextString" value="rekeyKey"/>
0034	<NameType type="Enumeration"
0035	value="UninterpretedTextString"/>
0036	</AttributeValue>
0037	</Attribute>
0038	</TemplateAttribute>
0039	</RequestPayload>
0040	</BatchItem>
0041	</RequestMessage>
0042	<ResponseMessage>
0043	<ResponseHeader>
0044	<ProtocolVersion>
0045	<ProtocolVersionMajor type="Integer" value="1"/>
0046	<ProtocolVersionMinor type="Integer" value="0"/>
0047	</ProtocolVersion>
0048	<TimeStamp type="DateTime" value="2010-02-11T14:12:24+00:00"/>
0049	<BatchCount type="Integer" value="1"/>
0050	</ResponseHeader>
0051	<BatchItem>
0052	<Operation type="Enumeration" value="Create"/>
0053	<ResultStatus type="Enumeration" value="Success"/>
0054	<ResponsePayload>
0055	<ObjectType type="Enumeration" value="SymmetricKey"/>
0056	<UniqueIdentifier type="TextString"
0057	value="\$UNIQUE_IDENTIFIER_0"/>
0058	</ResponsePayload>
0059	</BatchItem>
0060	</ResponseMessage>
0061	# TIME 1
0062	<RequestMessage>
0063	<RequestHeader>
0064	<ProtocolVersion>
	<ProtocolVersionMajor type="Integer" value="1"/>
	<ProtocolVersionMinor type="Integer" value="0"/>
	</ProtocolVersion>

0065	<BatchCount type="Integer" value="1"/>
0066	</RequestHeader>
0067	<BatchItem>
0068	<Operation type="Enumeration" value="GetAttributes"/>
0069	<RequestPayload>
0070	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0071	<AttributeName type="TextString" value="State"/>
0072	</RequestPayload>
0073	</BatchItem>
0074	</RequestMessage>
0075	<ResponseMessage>
0076	<ResponseHeader>
0077	<ProtocolVersion>
0078	<ProtocolVersionMajor type="Integer" value="1"/>
0079	<ProtocolVersionMinor type="Integer" value="0"/>
0080	</ProtocolVersion>
0081	<TimeStamp type="DateTime" value="2010-02-11T14:12:24+00:00"/>
0082	<BatchCount type="Integer" value="1"/>
0083	</ResponseHeader>
0084	<BatchItem>
0085	<Operation type="Enumeration" value="GetAttributes"/>
0086	<ResultStatus type="Enumeration" value="Success"/>
0087	<ResponsePayload>
0088	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0089	<Attribute>
0090	<AttributeName type="TextString" value="State"/>
0091	<AttributeValue type="Enumeration" value="Active"/>
0092	</Attribute>
0093	</ResponsePayload>
0094	</BatchItem>
0095	</ResponseMessage>
	# TIME 2
0096	<RequestMessage>
0097	<RequestHeader>
0098	<ProtocolVersion>
0099	<ProtocolVersionMajor type="Integer" value="1"/>
0100	<ProtocolVersionMinor type="Integer" value="0"/>
0101	</ProtocolVersion>
0102	<BatchCount type="Integer" value="1"/>
0103	</RequestHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Revoke"/>
0106	<RequestPayload>
0107	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0108	<RevocationReason>
0109	<RevocationReasonCode type="Enumeration"
	value="KeyCompromise"/>
0110	</RevocationReason>
0111	<CompromiseOccurrenceDate type="DateTime" value="2010-02-
	11T14:12:24+00:00"/>
0112	</RequestPayload>
0113	</BatchItem>
0114	</RequestMessage>

0115	<ResponseMessage>
0116	<ResponseHeader>
0117	<ProtocolVersion>
0118	<ProtocolVersionMajor type="Integer" value="1"/>
0119	<ProtocolVersionMinor type="Integer" value="0"/>
0120	</ProtocolVersion>
0121	<TimeStamp type="DateTime" value="2010-02-11T14:12:25+00:00"/>
0122	<BatchCount type="Integer" value="1"/>
0123	</ResponseHeader>
0124	<BatchItem>
0125	<Operation type="Enumeration" value="Revoke"/>
0126	<ResultStatus type="Enumeration" value="Success"/>
0127	<ResponsePayload>
0128	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0129	</ResponsePayload>
0130	</BatchItem>
0131	</ResponseMessage>
# TIME 3	
0132	<RequestMessage>
0133	<RequestHeader>
0134	<ProtocolVersion>
0135	<ProtocolVersionMajor type="Integer" value="1"/>
0136	<ProtocolVersionMinor type="Integer" value="0"/>
0137	</ProtocolVersion>
0138	<BatchCount type="Integer" value="1"/>
0139	</RequestHeader>
0140	<BatchItem>
0141	<Operation type="Enumeration" value="GetAttributes"/>
0142	<RequestPayload>
0143	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0144	<AttributeName type="TextString" value="State"/>
0145	</RequestPayload>
0146	</BatchItem>
0147	</RequestMessage>
0148	<ResponseMessage>
0149	<ResponseHeader>
0150	<ProtocolVersion>
0151	<ProtocolVersionMajor type="Integer" value="1"/>
0152	<ProtocolVersionMinor type="Integer" value="0"/>
0153	</ProtocolVersion>
0154	<TimeStamp type="DateTime" value="2010-02-11T14:12:25+00:00"/>
0155	<BatchCount type="Integer" value="1"/>
0156	</ResponseHeader>
0157	<BatchItem>
0158	<Operation type="Enumeration" value="GetAttributes"/>
0159	<ResultStatus type="Enumeration" value="Success"/>
0160	<ResponsePayload>
0161	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0162	<Attribute>
0163	<AttributeName type="TextString" value="State"/>
0164	<AttributeValue type="Enumeration" value="Compromised"/>
0165	</Attribute>
0166	</ResponsePayload>
0167	</BatchItem>

0168	</ResponseMessage>
	# TIME 4
0169	<RequestMessage>
0170	<RequestHeader>
0171	<ProtocolVersion>
0172	<ProtocolVersionMajor type="Integer" value="1"/>
0173	<ProtocolVersionMinor type="Integer" value="0"/>
0174	</ProtocolVersion>
0175	<BatchCount type="Integer" value="1"/>
0176	</RequestHeader>
0177	<BatchItem>
0178	<Operation type="Enumeration" value="ReKey"/>
0179	<RequestPayload>
0180	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0181	</RequestPayload>
0182	</BatchItem>
0183	</RequestMessage>
0184	<ResponseMessage>
0185	<ResponseHeader>
0186	<ProtocolVersion>
0187	<ProtocolVersionMajor type="Integer" value="1"/>
0188	<ProtocolVersionMinor type="Integer" value="0"/>
0189	</ProtocolVersion>
0190	<TimeStamp type="DateTime" value="2010-02-11T14:12:25+00:00"/>
0191	<BatchCount type="Integer" value="1"/>
0192	</ResponseHeader>
0193	<BatchItem>
0194	<Operation type="Enumeration" value="ReKey"/>
0195	<ResultStatus type="Enumeration" value="Success"/>
0196	<ResponsePayload>
0197	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0198	</ResponsePayload>
0199	</BatchItem>
0200	</ResponseMessage>
	# TIME 5
0201	<RequestMessage>
0202	<RequestHeader>
0203	<ProtocolVersion>
0204	<ProtocolVersionMajor type="Integer" value="1"/>
0205	<ProtocolVersionMinor type="Integer" value="0"/>
0206	</ProtocolVersion>
0207	<BatchCount type="Integer" value="1"/>
0208	</RequestHeader>
0209	<BatchItem>
0210	<Operation type="Enumeration" value="GetAttributes"/>
0211	<RequestPayload>
0212	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0213	<AttributeName type="TextString" value="State"/>
0214	</RequestPayload>
0215	</BatchItem>
0216	</RequestMessage>
0217	<ResponseMessage>
0218	<ResponseHeader>

0219	<ProtocolVersion>
0220	<ProtocolVersionMajor type="Integer" value="1"/>
0221	<ProtocolVersionMinor type="Integer" value="0"/>
0222	</ProtocolVersion>
0223	<TimeStamp type="DateTime" value="2010-02-11T14:12:25+00:00"/>
0224	<BatchCount type="Integer" value="1"/>
0225	</ResponseHeader>
0226	<BatchItem>
0227	<Operation type="Enumeration" value="GetAttributes"/>
0228	<ResultStatus type="Enumeration" value="Success"/>
0229	<ResponsePayload>
0230	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0231	<Attribute>
0232	<AttributeName type="TextString" value="State"/>
0233	<AttributeValue type="Enumeration" value="Active"/>
0234	</Attribute>
0235	</ResponsePayload>
0236	</BatchItem>
0237	</ResponseMessage>
# TIME 6	
0238	<RequestMessage>
0239	<RequestHeader>
0240	<ProtocolVersion>
0241	<ProtocolVersionMajor type="Integer" value="1"/>
0242	<ProtocolVersionMinor type="Integer" value="0"/>
0243	</ProtocolVersion>
0244	<BatchCount type="Integer" value="1"/>
0245	</RequestHeader>
0246	<BatchItem>
0247	<Operation type="Enumeration" value="Destroy"/>
0248	<RequestPayload>
0249	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0250	</RequestPayload>
0251	</BatchItem>
0252	</RequestMessage>
0253	<ResponseMessage>
0254	<ResponseHeader>
0255	<ProtocolVersion>
0256	<ProtocolVersionMajor type="Integer" value="1"/>
0257	<ProtocolVersionMinor type="Integer" value="0"/>
0258	</ProtocolVersion>
0259	<TimeStamp type="DateTime" value="2010-02-11T14:12:25+00:00"/>
0260	<BatchCount type="Integer" value="1"/>
0261	</ResponseHeader>
0262	<BatchItem>
0263	<Operation type="Enumeration" value="Destroy"/>
0264	<ResultStatus type="Enumeration" value="Success"/>
0265	<ResponsePayload>
0266	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0267	</ResponsePayload>
0268	</BatchItem>
0269	</ResponseMessage>
# TIME 7	

0270	<RequestMessage>
0271	<RequestHeader>
0272	<ProtocolVersion>
0273	<ProtocolVersionMajor type="Integer" value="1"/>
0274	<ProtocolVersionMinor type="Integer" value="0"/>
0275	</ProtocolVersion>
0276	<BatchOrderOption type="Boolean" value="true"/>
0277	<BatchCount type="Integer" value="2"/>
0278	</RequestHeader>
0279	<BatchItem>
0280	<Operation type="Enumeration" value="Revoke"/>
0281	<UniqueBatchItemID type="ByteString" value="7131695cf636735e"/>
0282	<RequestPayload>
0283	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0284	<RevocationReason>
0285	<RevocationReasonCode type="Enumeration"
	value="CessationOfOperation"/>
0286	</RevocationReason>
0287	</RequestPayload>
0288	</BatchItem>
0289	<BatchItem>
0290	<Operation type="Enumeration" value="Destroy"/>
0291	<UniqueBatchItemID type="ByteString" value="1845bcbbf09b5a66"/>
0292	<RequestPayload>
0293	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0294	</RequestPayload>
0295	</BatchItem>
0296	</RequestMessage>
0297	<ResponseMessage>
0298	<ResponseHeader>
0299	<ProtocolVersion>
0300	<ProtocolVersionMajor type="Integer" value="1"/>
0301	<ProtocolVersionMinor type="Integer" value="0"/>
0302	</ProtocolVersion>
0303	<TimeStamp type="DateTime" value="2010-02-11T14:12:25+00:00"/>
0304	<BatchCount type="Integer" value="2"/>
0305	</ResponseHeader>
0306	<BatchItem>
0307	<Operation type="Enumeration" value="Revoke"/>
0308	<UniqueBatchItemID type="ByteString" value="7131695cf636735e"/>
0309	<ResultStatus type="Enumeration" value="Success"/>
0310	<ResponsePayload>
0311	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0312	</ResponsePayload>
0313	</BatchItem>
0314	<BatchItem>
0315	<Operation type="Enumeration" value="Destroy"/>
0316	<UniqueBatchItemID type="ByteString" value="1845bcbbf09b5a66"/>
0317	<ResultStatus type="Enumeration" value="Success"/>
0318	<ResponsePayload>
0319	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0320	</ResponsePayload>
0321	</BatchItem>

0322	</ResponseMessage>
------	--------------------

161

162 2.1.17 TC-94-10 - Create Key, Re-key with New Life-cycle

163 Create a symmetric key with a specific name, then use Locate to find the key. After using Re-key
164 to create a new key, verify that the name was removed from the existing key and copied to the
165 new key. To clean up, both keys are deleted.

	<i># TIME 0</i>
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Length"/>
0022	<AttributeValue type="Integer" value="128"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Cryptographic
0026	Usage Mask"/>
0027	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="Name"/>
0031	<AttributeValue>
0032	<NameValue type="TextString" value="rekeyKey"/>
0033	<NameType type="Enumeration"
0034	value="UninterpretedTextString"/>
0035	</Attribute>
0036	</TemplateAttribute>
0037	</RequestPayload>
0038	</BatchItem>
0039	</RequestMessage>
0040	<ResponseMessage>
0041	<ResponseHeader>
0042	<ProtocolVersion>
	<ProtocolVersionMajor type="Integer" value="1"/>
	<ProtocolVersionMinor type="Integer" value="0"/>
	</ProtocolVersion>

0043	<TimeStamp type="DateTime" value="2010-02-11T15:38:29+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
# TIME 1	
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="0"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="Locate"/>
0065	<RequestPayload>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Name"/>
0068	<AttributeValue>
0069	<NameValue type="TextString" value="rekeyKey"/>
0070	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0071	</AttributeValue>
0072	</Attribute>
0073	</RequestPayload>
0074	</BatchItem>
0075	</RequestMessage>
0076	<ResponseMessage>
0077	<ResponseHeader>
0078	<ProtocolVersion>
0079	<ProtocolVersionMajor type="Integer" value="1"/>
0080	<ProtocolVersionMinor type="Integer" value="0"/>
0081	</ProtocolVersion>
0082	<TimeStamp type="DateTime" value="2010-02-11T15:38:30+00:00"/>
0083	<BatchCount type="Integer" value="1"/>
0084	</ResponseHeader>
0085	<BatchItem>
0086	<Operation type="Enumeration" value="Locate"/>
0087	<ResultStatus type="Enumeration" value="Success"/>
0088	<ResponsePayload>
0089	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0090	</ResponsePayload>
0091	</BatchItem>
0092	</ResponseMessage>
# TIME 2	
0093	<RequestMessage>

0094	<RequestHeader>
0095	<ProtocolVersion>
0096	<ProtocolVersionMajor type="Integer" value="1"/>
0097	<ProtocolVersionMinor type="Integer" value="0"/>
0098	</ProtocolVersion>
0099	<BatchCount type="Integer" value="1"/>
0100	</RequestHeader>
0101	<BatchItem>
0102	<Operation type="Enumeration" value="ReKey"/>
0103	<RequestPayload>
0104	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0105	<TemplateAttribute>
0106	<Attribute>
0107	<AttributeName type="TextString" value="Activation Date"/>
0108	<AttributeValue type="DateTime" value="2006-01-
	01T11:00:00+00:00"/>
0109	</Attribute>
0110	<Attribute>
0111	<AttributeName type="TextString" value="Process Start
	Date"/>
0112	<AttributeValue type="DateTime" value="2006-01-
	01T11:00:00+00:00"/>
0113	</Attribute>
0114	<Attribute>
0115	<AttributeName type="TextString" value="Protect Stop
	Date"/>
0116	<AttributeValue type="DateTime" value="2020-01-
	01T11:00:00+00:00"/>
0117	</Attribute>
0118	<Attribute>
0119	<AttributeName type="TextString" value="Deactivation
	Date"/>
0120	<AttributeValue type="DateTime" value="2020-01-
	01T11:00:00+00:00"/>
0121	</Attribute>
0122	</TemplateAttribute>
0123	</RequestPayload>
0124	</BatchItem>
0125	</RequestMessage>
0126	<ResponseMessage>
0127	<ResponseHeader>
0128	<ProtocolVersion>
0129	<ProtocolVersionMajor type="Integer" value="1"/>
0130	<ProtocolVersionMinor type="Integer" value="0"/>
0131	</ProtocolVersion>
0132	<TimeStamp type="DateTime" value="2010-02-11T15:38:31+00:00"/>
0133	<BatchCount type="Integer" value="1"/>
0134	</ResponseHeader>
0135	<BatchItem>
0136	<Operation type="Enumeration" value="ReKey"/>
0137	<ResultStatus type="Enumeration" value="Success"/>
0138	<ResponsePayload>
0139	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0140	</ResponsePayload>
0141	</BatchItem>

0142	</ResponseMessage>
	# TIME 3
0143	<RequestMessage>
0144	<RequestHeader>
0145	<ProtocolVersion>
0146	<ProtocolVersionMajor type="Integer" value="1"/>
0147	<ProtocolVersionMinor type="Integer" value="0"/>
0148	</ProtocolVersion>
0149	<BatchCount type="Integer" value="1"/>
0150	</RequestHeader>
0151	<BatchItem>
0152	<Operation type="Enumeration" value="GetAttributes"/>
0153	<RequestPayload>
0154	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0155	<AttributeName type="TextString" value="Name"/>
0156	</RequestPayload>
0157	</BatchItem>
0158	</RequestMessage>
0159	<ResponseMessage>
0160	<ResponseHeader>
0161	<ProtocolVersion>
0162	<ProtocolVersionMajor type="Integer" value="1"/>
0163	<ProtocolVersionMinor type="Integer" value="0"/>
0164	</ProtocolVersion>
0165	<TimeStamp type="DateTime" value="2010-02-11T15:38:31+00:00"/>
0166	<BatchCount type="Integer" value="1"/>
0167	</ResponseHeader>
0168	<BatchItem>
0169	<Operation type="Enumeration" value="GetAttributes"/>
0170	<ResultStatus type="Enumeration" value="Success"/>
0171	<ResponsePayload>
0172	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0173	</ResponsePayload>
0174	</BatchItem>
0175	</ResponseMessage>
	# TIME 4
0176	<RequestMessage>
0177	<RequestHeader>
0178	<ProtocolVersion>
0179	<ProtocolVersionMajor type="Integer" value="1"/>
0180	<ProtocolVersionMinor type="Integer" value="0"/>
0181	</ProtocolVersion>
0182	<BatchCount type="Integer" value="1"/>
0183	</RequestHeader>
0184	<BatchItem>
0185	<Operation type="Enumeration" value="GetAttributes"/>
0186	<RequestPayload>
0187	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0188	<AttributeName type="TextString" value="Activation Date"/>
0189	<AttributeName type="TextString" value="Process Start Date"/>
0190	<AttributeName type="TextString" value="Protect Stop Date"/>
0191	<AttributeName type="TextString" value="Deactivation Date"/>
0192	</RequestPayload>

0193	</BatchItem>
0194	</RequestMessage>
0195	<ResponseMessage>
0196	<ResponseHeader>
0197	<ProtocolVersion>
0198	<ProtocolVersionMajor type="Integer" value="1"/>
0199	<ProtocolVersionMinor type="Integer" value="0"/>
0200	</ProtocolVersion>
0201	<TimeStamp type="DateTime" value="2010-02-11T15:38:31+00:00"/>
0202	<BatchCount type="Integer" value="1"/>
0203	</ResponseHeader>
0204	<BatchItem>
0205	<Operation type="Enumeration" value="GetAttributes"/>
0206	<ResultStatus type="Enumeration" value="Success"/>
0207	<ResponsePayload>
0208	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0209	<Attribute>
0210	<AttributeName type="TextString" value="Activation Date"/>
0211	<AttributeValue type="DateTime" value="2006-01-
	01T11:00:00+00:00"/>
0212	</Attribute>
0213	<Attribute>
0214	<AttributeName type="TextString" value="Process Start
	Date"/>
0215	<AttributeValue type="DateTime" value="2006-01-
	01T11:00:00+00:00"/>
0216	</Attribute>
0217	<Attribute>
0218	<AttributeName type="TextString" value="Protect Stop Date"/>
0219	<AttributeValue type="DateTime" value="2020-01-
	01T11:00:00+00:00"/>
0220	</Attribute>
0221	<Attribute>
0222	<AttributeName type="TextString" value="Deactivation Date"/>
0223	<AttributeValue type="DateTime" value="2020-01-
	01T11:00:00+00:00"/>
0224	</Attribute>
0225	</ResponsePayload>
0226	</BatchItem>
0227	</ResponseMessage>
	# TIME 5
0228	<RequestMessage>
0229	<RequestHeader>
0230	<ProtocolVersion>
0231	<ProtocolVersionMajor type="Integer" value="1"/>
0232	<ProtocolVersionMinor type="Integer" value="0"/>
0233	</ProtocolVersion>
0234	<BatchCount type="Integer" value="1"/>
0235	</RequestHeader>
0236	<BatchItem>
0237	<Operation type="Enumeration" value="Locate"/>
0238	<RequestPayload>
0239	<Attribute>
0240	<AttributeName type="TextString" value="Name"/>
0241	<AttributeValue>
0242	<NameValue type="TextString" value="rekeyKey"/>

0243	<NameType type="Enumeration"
0244	value="UninterpretedTextString"/>
0245	</Attribute>
0246	</RequestPayload>
0247	</BatchItem>
0248	</RequestMessage>
0249	<ResponseMessage>
0250	<ResponseHeader>
0251	<ProtocolVersion>
0252	<ProtocolVersionMajor type="Integer" value="1"/>
0253	<ProtocolVersionMinor type="Integer" value="0"/>
0254	</ProtocolVersion>
0255	<TimeStamp type="DateTime" value="2010-02-11T15:38:31+00:00"/>
0256	<BatchCount type="Integer" value="1"/>
0257	</ResponseHeader>
0258	<BatchItem>
0259	<Operation type="Enumeration" value="Locate"/>
0260	<ResultStatus type="Enumeration" value="Success"/>
0261	<ResponsePayload>
0262	<UniqueIdentifier type="TextString"
0263	value="\$UNIQUE_IDENTIFIER_1"/>
0264	</ResponsePayload>
0265	</BatchItem>
0266	</ResponseMessage>
0266	# TIME 6
0267	<RequestMessage>
0268	<RequestHeader>
0269	<ProtocolVersion>
0270	<ProtocolVersionMajor type="Integer" value="1"/>
0271	<ProtocolVersionMinor type="Integer" value="0"/>
0272	</ProtocolVersion>
0273	<BatchCount type="Integer" value="1"/>
0274	</RequestHeader>
0275	<BatchItem>
0276	<Operation type="Enumeration" value="Destroy"/>
0277	<RequestPayload>
0278	<UniqueIdentifier type="TextString"
0279	value="\$UNIQUE_IDENTIFIER_0"/>
0280	</RequestPayload>
0281	</BatchItem>
0282	</RequestMessage>
0283	<ResponseMessage>
0284	<ResponseHeader>
0285	<ProtocolVersion>
0286	<ProtocolVersionMajor type="Integer" value="1"/>
0287	<ProtocolVersionMinor type="Integer" value="0"/>
0288	</ProtocolVersion>
0289	<TimeStamp type="DateTime" value="2010-02-11T15:38:32+00:00"/>
0290	<BatchCount type="Integer" value="1"/>
0291	</ResponseHeader>
0292	<BatchItem>
0293	<Operation type="Enumeration" value="Destroy"/>
0294	<ResultStatus type="Enumeration" value="Success"/>
0295	<ResponsePayload>
0296	<UniqueIdentifier type="TextString"

0295	value="\$UNIQUE_IDENTIFIER_0"/>
0296	</ResponsePayload>
0297	</BatchItem>
0297	</ResponseMessage>
0298	# TIME 7
0298	<RequestMessage>
0299	<RequestHeader>
0300	<ProtocolVersion>
0301	<ProtocolVersionMajor type="Integer" value="1"/>
0302	<ProtocolVersionMinor type="Integer" value="0"/>
0303	</ProtocolVersion>
0304	<BatchOrderOption type="Boolean" value="true"/>
0305	<BatchCount type="Integer" value="2"/>
0306	</RequestHeader>
0307	<BatchItem>
0308	<Operation type="Enumeration" value="Revoke"/>
0309	<UniqueBatchItemID type="ByteString" value="3dc816bb39869d07"/>
0310	<RequestPayload>
0311	<UniqueIdentifier type="TextString"
0312	value="\$UNIQUE_IDENTIFIER_1"/>
0312	<RevocationReason>
0313	<RevocationReasonCode type="Enumeration"
0314	value="CessationOfOperation"/>
0314	</RevocationReason>
0315	</RequestPayload>
0316	</BatchItem>
0317	<BatchItem>
0318	<Operation type="Enumeration" value="Destroy"/>
0319	<UniqueBatchItemID type="ByteString" value="32b517312fd5b558"/>
0320	<RequestPayload>
0321	<UniqueIdentifier type="TextString"
0322	value="\$UNIQUE_IDENTIFIER_1"/>
0322	</RequestPayload>
0323	</BatchItem>
0324	</RequestMessage>
0325	<ResponseMessage>
0326	<ResponseHeader>
0327	<ProtocolVersion>
0328	<ProtocolVersionMajor type="Integer" value="1"/>
0329	<ProtocolVersionMinor type="Integer" value="0"/>
0330	</ProtocolVersion>
0331	<TimeStamp type="DateTime" value="2010-02-11T15:38:32+00:00"/>
0332	<BatchCount type="Integer" value="2"/>
0333	</ResponseHeader>
0334	<BatchItem>
0335	<Operation type="Enumeration" value="Revoke"/>
0336	<UniqueBatchItemID type="ByteString" value="3dc816bb39869d07"/>
0337	<ResultStatus type="Enumeration" value="Success"/>
0338	<ResponsePayload>
0339	<UniqueIdentifier type="TextString"
0340	value="\$UNIQUE_IDENTIFIER_1"/>
0340	</ResponsePayload>
0341	</BatchItem>
0342	<BatchItem>
0343	<Operation type="Enumeration" value="Destroy"/>
0344	<UniqueBatchItemID type="ByteString" value="32b517312fd5b558"/>
0345	<ResultStatus type="Enumeration" value="Success"/>

0346	<ResponsePayload>
0347	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0348	</ResponsePayload>
0349	</BatchItem>
0350	</ResponseMessage>

166

167 2.1.18 TC-95-10 - Obtain Lease for Expired Key

168 Create a symmetric key with a specific name and obtain a lease. Revoke the key with state
169 'Compromised' and re-key the key. Try to obtain a lease on the old key which fails due to a
170 server policy which does not allow giving out leases for compromised keys. Locate the new key
171 with the original name. Get the new key and obtain a lease.

	# TIME 0
	# [Client-A]
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="rekeyKey"/>
0030	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0031	</AttributeValue>
0032	</Attribute>
0033	<Attribute>
0034	<AttributeName type="TextString" value="Activation Date"/>

0035	<AttributeValue type="DateTime" value="2010-02-11T15:45:48+00:00"/>
0036	</Attribute>
0037	</TemplateAttribute>
0038	</RequestPayload>
0039	</BatchItem>
0040	</RequestMessage>
0041	<ResponseMessage>
0042	<ResponseHeader>
0043	<ProtocolVersion>
0044	<ProtocolVersionMajor type="Integer" value="1"/>
0045	<ProtocolVersionMinor type="Integer" value="0"/>
0046	</ProtocolVersion>
0047	<TimeStamp type="DateTime" value="2010-02-11T15:45:49+00:00"/>
0048	<BatchCount type="Integer" value="1"/>
0049	</ResponseHeader>
0050	<BatchItem>
0051	<Operation type="Enumeration" value="Create"/>
0052	<ResultStatus type="Enumeration" value="Success"/>
0053	<ResponsePayload>
0054	<ObjectType type="Enumeration" value="SymmetricKey"/>
0055	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0056	</ResponsePayload>
0057	</BatchItem>
0058	</ResponseMessage>
	# TIME 1
	# [Client-A]
0059	<RequestMessage>
0060	<RequestHeader>
0061	<ProtocolVersion>
0062	<ProtocolVersionMajor type="Integer" value="1"/>
0063	<ProtocolVersionMinor type="Integer" value="0"/>
0064	</ProtocolVersion>
0065	<BatchCount type="Integer" value="1"/>
0066	</RequestHeader>
0067	<BatchItem>
0068	<Operation type="Enumeration" value="Get"/>
0069	<RequestPayload>
0070	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0071	</RequestPayload>
0072	</BatchItem>
0073	</RequestMessage>
0074	<ResponseMessage>
0075	<ResponseHeader>
0076	<ProtocolVersion>
0077	<ProtocolVersionMajor type="Integer" value="1"/>
0078	<ProtocolVersionMinor type="Integer" value="0"/>
0079	</ProtocolVersion>
0080	<TimeStamp type="DateTime" value="2010-02-11T15:45:49+00:00"/>
0081	<BatchCount type="Integer" value="1"/>
0082	</ResponseHeader>
0083	<BatchItem>
0084	<Operation type="Enumeration" value="Get"/>
0085	<ResultStatus type="Enumeration" value="Success"/>

0086	<ResponsePayload>
0087	<ObjectType type="Enumeration" value="SymmetricKey"/>
0088	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0089	<SymmetricKey>
0090	<KeyBlock>
0091	<KeyFormatType type="Enumeration" value="Raw"/>
0092	<KeyValue>
0093	<KeyMaterial type="ByteString"
	value="f43c7798aacb22b1411a8773c199708b"/>
0094	</KeyValue>
0095	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0096	<CryptographicLength type="Integer" value="128"/>
0097	</KeyBlock>
0098	</SymmetricKey>
0099	</ResponsePayload>
0100	</BatchItem>
0101	</ResponseMessage>
	# TIME 2
	# [Client-A]
0102	<RequestMessage>
0103	<RequestHeader>
0104	<ProtocolVersion>
0105	<ProtocolVersionMajor type="Integer" value="1"/>
0106	<ProtocolVersionMinor type="Integer" value="0"/>
0107	</ProtocolVersion>
0108	<BatchCount type="Integer" value="1"/>
0109	</RequestHeader>
0110	<BatchItem>
0111	<Operation type="Enumeration" value="ObtainLease"/>
0112	<RequestPayload>
0113	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0114	</RequestPayload>
0115	</BatchItem>
0116	</RequestMessage>
0117	<ResponseMessage>
0118	<ResponseHeader>
0119	<ProtocolVersion>
0120	<ProtocolVersionMajor type="Integer" value="1"/>
0121	<ProtocolVersionMinor type="Integer" value="0"/>
0122	</ProtocolVersion>
0123	<TimeStamp type="DateTime" value="2010-02-11T15:45:50+00:00"/>
0124	<BatchCount type="Integer" value="1"/>
0125	</ResponseHeader>
0126	<BatchItem>
0127	<Operation type="Enumeration" value="ObtainLease"/>
0128	<ResultStatus type="Enumeration" value="Success"/>
0129	<ResponsePayload>
0130	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0131	<LeaseTime type="Interval" value="16"/>
0132	<LastChangeDate type="DateTime" value="2010-02-11T15:45:49+00:00"/>
0133	</ResponsePayload>
0134	</BatchItem>
0135	</ResponseMessage>

0136	# TIME 3
0137	# [Client-B]
0138	<RequestMessage>
0139	<RequestHeader>
0140	<ProtocolVersion>
0141	<ProtocolVersionMajor type="Integer" value="1"/>
0142	<ProtocolVersionMinor type="Integer" value="0"/>
0143	</ProtocolVersion>
0144	<BatchCount type="Integer" value="1"/>
0145	</BatchCount>
0146	<BatchItem>
0147	<Operation type="Enumeration" value="Revoke"/>
0148	<RequestPayload>
0149	<UniqueIdentifier type="TextString"
0150	value="\$UNIQUE_IDENTIFIER_0"/>
0151	<RevocationReason>
0152	<RevocationReasonCode type="Enumeration"
0153	value="KeyCompromise"/>
0154	</RevocationReason>
0155	<CompromiseOccurrenceDate type="DateTime" value="2010-02-
0156	11T15:45:50+00:00"/>
0157	</RequestPayload>
0158	</BatchItem>
0159	</RequestMessage>
0160	<ResponseMessage>
0161	<ResponseHeader>
0162	<ProtocolVersion>
0163	<ProtocolVersionMajor type="Integer" value="1"/>
0164	<ProtocolVersionMinor type="Integer" value="0"/>
0165	</ProtocolVersion>
0166	<TimeStamp type="DateTime" value="2010-02-11T15:45:50+00:00"/>
0167	<BatchCount type="Integer" value="1"/>
0168	</BatchCount>
0169	<BatchItem>
0170	<Operation type="Enumeration" value="Revoke"/>
0171	<ResultStatus type="Enumeration" value="Success"/>
0172	<ResponsePayload>
0173	<UniqueIdentifier type="TextString"
0174	value="\$UNIQUE_IDENTIFIER_0"/>
0175	</ResponsePayload>
0176	</BatchItem>
0177	</ResponseMessage>
0178	# TIME 4
0179	# [Client-B]
0180	<RequestMessage>
0181	<RequestHeader>
0182	<ProtocolVersion>
0183	<ProtocolVersionMajor type="Integer" value="1"/>
0184	<ProtocolVersionMinor type="Integer" value="0"/>
0185	</ProtocolVersion>
0186	<BatchCount type="Integer" value="1"/>
0187	</BatchCount>
0188	<BatchItem>
0189	<Operation type="Enumeration" value="ReKey"/>
0190	<RequestPayload>
0191	<UniqueIdentifier type="TextString"
0192	value="\$UNIQUE_IDENTIFIER_0"/>

0184	</RequestPayload>
0185	</BatchItem>
0186	</RequestMessage>
0187	<ResponseMessage>
0188	<ResponseHeader>
0189	<ProtocolVersion>
0190	<ProtocolVersionMajor type="Integer" value="1"/>
0191	<ProtocolVersionMinor type="Integer" value="0"/>
0192	</ProtocolVersion>
0193	<TimeStamp type="DateTime" value="2010-02-11T15:45:51+00:00"/>
0194	<BatchCount type="Integer" value="1"/>
0195	</ResponseHeader>
0196	<BatchItem>
0197	<Operation type="Enumeration" value="ReKey"/>
0198	<ResultStatus type="Enumeration" value="Success"/>
0199	<ResponsePayload>
0200	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0201	</ResponsePayload>
0202	</BatchItem>
0203	</ResponseMessage>
	# TIME 5
	# [Client-A]
0204	<RequestMessage>
0205	<RequestHeader>
0206	<ProtocolVersion>
0207	<ProtocolVersionMajor type="Integer" value="1"/>
0208	<ProtocolVersionMinor type="Integer" value="0"/>
0209	</ProtocolVersion>
0210	<BatchCount type="Integer" value="1"/>
0211	</RequestHeader>
0212	<BatchItem>
0213	<Operation type="Enumeration" value="ObtainLease"/>
0214	<RequestPayload>
0215	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0216	</RequestPayload>
0217	</BatchItem>
0218	</RequestMessage>
0219	<ResponseMessage>
0220	<ResponseHeader>
0221	<ProtocolVersion>
0222	<ProtocolVersionMajor type="Integer" value="1"/>
0223	<ProtocolVersionMinor type="Integer" value="0"/>
0224	</ProtocolVersion>
0225	<TimeStamp type="DateTime" value="2010-02-11T15:45:51+00:00"/>
0226	<BatchCount type="Integer" value="1"/>
0227	</ResponseHeader>
0228	<BatchItem>
0229	<Operation type="Enumeration" value="ObtainLease"/>
0230	<ResultStatus type="Enumeration" value="OperationFailed"/>
0231	<ResultReason type="Enumeration" value="PermissionDenied"/>
0232	<ResultMessage type="TextString" value="CO is in state
	Compromised, no lease given"/>
0233	</BatchItem>
0234	</ResponseMessage>

0235	# TIME 6
0236	# [Client-A]
0237	<RequestMessage>
0238	<RequestHeader>
0239	<ProtocolVersion>
0240	<ProtocolVersionMajor type="Integer" value="1"/>
0241	<ProtocolVersionMinor type="Integer" value="0"/>
0242	</ProtocolVersion>
0243	<BatchCount type="Integer" value="1"/>
0244	</BatchCount>
0245	<Operation type="Enumeration" value="Locate"/>
0246	<RequestPayload>
0247	<Attribute>
0248	<AttributeName type="TextString" value="Name"/>
0249	<AttributeValue>
0250	<NameValue type="TextString" value="rekeyKey"/>
0251	<NameType type="Enumeration"
0252	value="UninterpretedTextString"/>
0253	</NameType>
0254	</AttributeValue>
0255	</Attribute>
0256	</RequestPayload>
0257	</BatchItem>
0258	</RequestMessage>
0259	<ResponseMessage>
0260	<ResponseHeader>
0261	<ProtocolVersion>
0262	<ProtocolVersionMajor type="Integer" value="1"/>
0263	<ProtocolVersionMinor type="Integer" value="0"/>
0264	</ProtocolVersion>
0265	<TimeStamp type="DateTime" value="2010-02-11T15:45:51+00:00"/>
0266	<BatchCount type="Integer" value="1"/>
0267	</BatchCount>
0268	<Operation type="Enumeration" value="Locate"/>
0269	<ResultStatus type="Enumeration" value="Success"/>
0270	<ResponsePayload>
0271	<UniqueIdentifier type="TextString"
0272	value="\$UNIQUE_IDENTIFIER_1"/>
0273	</UniqueIdentifier>
0274	</ResponsePayload>
0275	</BatchItem>
0276	</ResponseMessage>
0277	# TIME 7
0278	# [Client-A]
0279	<RequestMessage>
0280	<RequestHeader>
0281	<ProtocolVersion>
0282	<ProtocolVersionMajor type="Integer" value="1"/>
0283	<ProtocolVersionMinor type="Integer" value="0"/>
0284	</ProtocolVersion>
0285	<BatchCount type="Integer" value="1"/>
0286	</BatchCount>
0287	<Operation type="Enumeration" value="Get"/>
0288	<RequestPayload>
0289	<UniqueIdentifier type="TextString"
0290	value="\$UNIQUE_IDENTIFIER_1"/>
0291	</UniqueIdentifier>
0292	</RequestPayload>
0293	</BatchItem>
0294	</RequestMessage>

0285	</RequestPayload>
0286	</BatchItem>
0287	</RequestMessage>
0288	<ResponseMessage>
0289	<ResponseHeader>
0290	<ProtocolVersion>
0291	<ProtocolVersionMajor type="Integer" value="1"/>
0292	<ProtocolVersionMinor type="Integer" value="0"/>
0293	</ProtocolVersion>
0294	<TimeStamp type="DateTime" value="2010-02-11T15:45:51+00:00"/>
0295	<BatchCount type="Integer" value="1"/>
0296	</ResponseHeader>
0297	<BatchItem>
0298	<Operation type="Enumeration" value="Get"/>
0299	<ResultStatus type="Enumeration" value="Success"/>
0300	<ResponsePayload>
0301	<ObjectType type="Enumeration" value="SymmetricKey"/>
0302	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0303	<SymmetricKey>
0304	<KeyBlock>
0305	<KeyFormatType type="Enumeration" value="Raw"/>
0306	<KeyValue>
0307	<KeyMaterial type="ByteString"
	value="173e9499f7c573712afb9883b5df2bce"/>
0308	</KeyValue>
0309	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0310	<CryptographicLength type="Integer" value="128"/>
0311	</KeyBlock>
0312	</SymmetricKey>
0313	</ResponsePayload>
0314	</BatchItem>
0315	</ResponseMessage>
	# TIME 8
	# [Client-A]
0316	<RequestMessage>
0317	<RequestHeader>
0318	<ProtocolVersion>
0319	<ProtocolVersionMajor type="Integer" value="1"/>
0320	<ProtocolVersionMinor type="Integer" value="0"/>
0321	</ProtocolVersion>
0322	<BatchCount type="Integer" value="1"/>
0323	</RequestHeader>
0324	<BatchItem>
0325	<Operation type="Enumeration" value="ObtainLease"/>
0326	<RequestPayload>
0327	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0328	</RequestPayload>
0329	</BatchItem>
0330	</RequestMessage>
0331	<ResponseMessage>
0332	<ResponseHeader>
0333	<ProtocolVersion>
0334	<ProtocolVersionMajor type="Integer" value="1"/>
0335	<ProtocolVersionMinor type="Integer" value="0"/>

0336	</ProtocolVersion>
0337	<TimeStamp type="DateTime" value="2010-02-11T15:45:51+00:00"/>
0338	<BatchCount type="Integer" value="1"/>
0339	</ResponseHeader>
0340	<BatchItem>
0341	<Operation type="Enumeration" value="ObtainLease"/>
0342	<ResultStatus type="Enumeration" value="Success"/>
0343	<ResponsePayload>
0344	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0345	<LeaseTime type="Interval" value="0"/>
0346	<LastChangeDate type="DateTime" value="2010-02-
	11T15:45:51+00:00"/>
0347	</ResponsePayload>
0348	</BatchItem>
0349	</ResponseMessage>
	# TIME 9
	# [Client-A]
0350	<RequestMessage>
0351	<RequestHeader>
0352	<ProtocolVersion>
0353	<ProtocolVersionMajor type="Integer" value="1"/>
0354	<ProtocolVersionMinor type="Integer" value="0"/>
0355	</ProtocolVersion>
0356	<BatchCount type="Integer" value="1"/>
0357	</RequestHeader>
0358	<BatchItem>
0359	<Operation type="Enumeration" value="Destroy"/>
0360	<RequestPayload>
0361	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0362	</RequestPayload>
0363	</BatchItem>
0364	</RequestMessage>
0365	<ResponseMessage>
0366	<ResponseHeader>
0367	<ProtocolVersion>
0368	<ProtocolVersionMajor type="Integer" value="1"/>
0369	<ProtocolVersionMinor type="Integer" value="0"/>
0370	</ProtocolVersion>
0371	<TimeStamp type="DateTime" value="2010-02-11T15:45:51+00:00"/>
0372	<BatchCount type="Integer" value="1"/>
0373	</ResponseHeader>
0374	<BatchItem>
0375	<Operation type="Enumeration" value="Destroy"/>
0376	<ResultStatus type="Enumeration" value="Success"/>
0377	<ResponsePayload>
0378	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0379	</ResponsePayload>
0380	</BatchItem>
0381	</ResponseMessage>
	# TIME 10
	# [Client-A]
0382	<RequestMessage>
0383	<RequestHeader>

0384	<ProtocolVersion>
0385	<ProtocolVersionMajor type="Integer" value="1"/>
0386	<ProtocolVersionMinor type="Integer" value="0"/>
0387	</ProtocolVersion>
0388	<BatchOrderOption type="Boolean" value="true"/>
0389	<BatchCount type="Integer" value="2"/>
0390	</RequestHeader>
0391	<BatchItem>
0392	<Operation type="Enumeration" value="Revoke"/>
0393	<UniqueBatchItemID type="ByteString" value="3748b9e243205ba7"/>
0394	<RequestPayload>
0395	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0396	<RevocationReason>
0397	<RevocationReasonCode type="Enumeration"
	value="CessationOfOperation"/>
0398	</RevocationReason>
0399	</RequestPayload>
0400	</BatchItem>
0401	<BatchItem>
0402	<Operation type="Enumeration" value="Destroy"/>
0403	<UniqueBatchItemID type="ByteString" value="04eaf416d0beb50d"/>
0404	<RequestPayload>
0405	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0406	</RequestPayload>
0407	</BatchItem>
0408	</RequestMessage>
0409	<ResponseMessage>
0410	<ResponseHeader>
0411	<ProtocolVersion>
0412	<ProtocolVersionMajor type="Integer" value="1"/>
0413	<ProtocolVersionMinor type="Integer" value="0"/>
0414	</ProtocolVersion>
0415	<TimeStamp type="DateTime" value="2010-02-11T15:45:51+00:00"/>
0416	<BatchCount type="Integer" value="2"/>
0417	</ResponseHeader>
0418	<BatchItem>
0419	<Operation type="Enumeration" value="Revoke"/>
0420	<UniqueBatchItemID type="ByteString" value="3748b9e243205ba7"/>
0421	<ResultStatus type="Enumeration" value="Success"/>
0422	<ResponsePayload>
0423	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0424	</ResponsePayload>
0425	</BatchItem>
0426	<BatchItem>
0427	<Operation type="Enumeration" value="Destroy"/>
0428	<UniqueBatchItemID type="ByteString" value="04eaf416d0beb50d"/>
0429	<ResultStatus type="Enumeration" value="Success"/>
0430	<ResponsePayload>
0431	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0432	</ResponsePayload>
0433	</BatchItem>
0434	</ResponseMessage>

172

173 2.1.19 TC-101-10 - Create a Key, Archive and Recover it

174 Create a symmetric key with a specified name, then use Locate to find the key and get the key.
175 Archive the key (asynchronous operation, use Poll until it completes) and use Get and Locate on
176 it, but both fail. Add the Storage Status Mask to the Locate-command, indicating to the server to
177 search in both online and archived storage. The Locate finds the key. Recover the key from the
178 archive (also asynchronous), both Locate and Get succeed.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Length"/>
0022	<AttributeValue type="Integer" value="128"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Cryptographic
0026	Usage Mask"/>
0027	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="Name"/>
0031	<AttributeValue>
0032	<NameValue type="TextString" value="archiveKey"/>
0033	<NameType type="Enumeration"
0034	value="UninterpretedTextString"/>
0035	</AttributeValue>
0036	</Attribute>
0037	</TemplateAttribute>
0038	</RequestPayload>
0039	</BatchItem>
0040	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>

0041	<ProtocolVersionMinor type="Integer" value="0"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2010-02-12T09:30:11+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
# TIME 1	
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="0"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="Locate"/>
0065	<RequestPayload>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Object Type"/>
0068	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Name"/>
0072	<AttributeValue>
0073	<NameValue type="TextString" value="archiveKey"/>
0074	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0075	</AttributeValue>
0076	</Attribute>
0077	</RequestPayload>
0078	</BatchItem>
0079	</RequestMessage>
0080	<ResponseMessage>
0081	<ResponseHeader>
0082	<ProtocolVersion>
0083	<ProtocolVersionMajor type="Integer" value="1"/>
0084	<ProtocolVersionMinor type="Integer" value="0"/>
0085	</ProtocolVersion>
0086	<TimeStamp type="DateTime" value="2010-02-12T09:30:14+00:00"/>
0087	<BatchCount type="Integer" value="1"/>
0088	</ResponseHeader>
0089	<BatchItem>
0090	<Operation type="Enumeration" value="Locate"/>
0091	<ResultStatus type="Enumeration" value="Success"/>
0092	<ResponsePayload>
0093	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0094	</ResponsePayload>
0095	</BatchItem>
0096	</ResponseMessage>
# TIME 2	
0097	<RequestMessage>
0098	<RequestHeader>
0099	<ProtocolVersion>
0100	<ProtocolVersionMajor type="Integer" value="1"/>
0101	<ProtocolVersionMinor type="Integer" value="0"/>
0102	</ProtocolVersion>
0103	<BatchCount type="Integer" value="1"/>
0104	</RequestHeader>
0105	<BatchItem>
0106	<Operation type="Enumeration" value="Get"/>
0107	<RequestPayload>
0108	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0109	</RequestPayload>
0110	</BatchItem>
0111	</RequestMessage>
0112	<ResponseMessage>
0113	<ResponseHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="0"/>
0117	</ProtocolVersion>
0118	<TimeStamp type="DateTime" value="2010-02-12T09:30:15+00:00"/>
0119	<BatchCount type="Integer" value="1"/>
0120	</ResponseHeader>
0121	<BatchItem>
0122	<Operation type="Enumeration" value="Get"/>
0123	<ResultStatus type="Enumeration" value="Success"/>
0124	<ResponsePayload>
0125	<ObjectType type="Enumeration" value="SymmetricKey"/>
0126	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0127	<SymmetricKey>
0128	<KeyBlock>
0129	<KeyFormatType type="Enumeration" value="Raw"/>
0130	<KeyValue>
0131	<KeyMaterial type="ByteString"
	value="c3200b1291ba648db9089ded3073de74"/>
0132	</KeyValue>
0133	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0134	<CryptographicLength type="Integer" value="128"/>
0135	</KeyBlock>
0136	</SymmetricKey>
0137	</ResponsePayload>
0138	</BatchItem>
0139	</ResponseMessage>
# TIME 3	
0140	<RequestMessage>
0141	<RequestHeader>
0142	<ProtocolVersion>
0143	<ProtocolVersionMajor type="Integer" value="1"/>
0144	<ProtocolVersionMinor type="Integer" value="0"/>

0145	</ProtocolVersion>
0146	<AsynchronousIndicator type="Boolean" value="true"/>
0147	<BatchCount type="Integer" value="1"/>
0148	</RequestHeader>
0149	<BatchItem>
0150	<Operation type="Enumeration" value="Archive"/>
0151	<RequestPayload>
0152	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0153	</RequestPayload>
0154	</BatchItem>
0155	</RequestMessage>
0156	<ResponseMessage>
0157	<ResponseHeader>
0158	<ProtocolVersion>
0159	<ProtocolVersionMajor type="Integer" value="1"/>
0160	<ProtocolVersionMinor type="Integer" value="0"/>
0161	</ProtocolVersion>
0162	<TimeStamp type="DateTime" value="2010-02-12T09:30:15+00:00"/>
0163	<BatchCount type="Integer" value="1"/>
0164	</ResponseHeader>
0165	<BatchItem>
0166	<Operation type="Enumeration" value="Archive"/>
0167	<ResultStatus type="Enumeration" value="OperationPending"/>
0168	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0169	</BatchItem>
0170	</ResponseMessage>
	# TIME 4
0171	<RequestMessage>
0172	<RequestHeader>
0173	<ProtocolVersion>
0174	<ProtocolVersionMajor type="Integer" value="1"/>
0175	<ProtocolVersionMinor type="Integer" value="0"/>
0176	</ProtocolVersion>
0177	<BatchCount type="Integer" value="1"/>
0178	</RequestHeader>
0179	<BatchItem>
0180	<Operation type="Enumeration" value="Poll"/>
0181	<RequestPayload>
0182	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0183	</RequestPayload>
0184	</BatchItem>
0185	</RequestMessage>
0186	<ResponseMessage>
0187	<ResponseHeader>
0188	<ProtocolVersion>
0189	<ProtocolVersionMajor type="Integer" value="1"/>
0190	<ProtocolVersionMinor type="Integer" value="0"/>
0191	</ProtocolVersion>
0192	<TimeStamp type="DateTime" value="2010-02-12T09:30:18+00:00"/>
0193	<BatchCount type="Integer" value="1"/>
0194	</ResponseHeader>
0195	<BatchItem>
0196	<Operation type="Enumeration" value="Archive"/>

0197	<ResultStatus type="Enumeration" value="Success"/>
0198	<ResponsePayload>
0199	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0200	</ResponsePayload>
0201	</BatchItem>
0202	</ResponseMessage>
# TIME 5	
0203	<RequestMessage>
0204	<RequestHeader>
0205	<ProtocolVersion>
0206	<ProtocolVersionMajor type="Integer" value="1"/>
0207	<ProtocolVersionMinor type="Integer" value="0"/>
0208	</ProtocolVersion>
0209	<BatchCount type="Integer" value="1"/>
0210	</RequestHeader>
0211	<BatchItem>
0212	<Operation type="Enumeration" value="Get"/>
0213	<RequestPayload>
0214	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0215	</RequestPayload>
0216	</BatchItem>
0217	</RequestMessage>
0218	<ResponseMessage>
0219	<ResponseHeader>
0220	<ProtocolVersion>
0221	<ProtocolVersionMajor type="Integer" value="1"/>
0222	<ProtocolVersionMinor type="Integer" value="0"/>
0223	</ProtocolVersion>
0224	<TimeStamp type="DateTime" value="2010-02-12T09:30:20+00:00"/>
0225	<BatchCount type="Integer" value="1"/>
0226	</ResponseHeader>
0227	<BatchItem>
0228	<Operation type="Enumeration" value="Get"/>
0229	<ResultStatus type="Enumeration" value="OperationFailed"/>
0230	<ResultReason type="Enumeration" value="ObjectArchived"/>
0231	<ResultMessage type="TextString" value="Object is archived"/>
0232	</BatchItem>
0233	</ResponseMessage>
# TIME 6	
0234	<RequestMessage>
0235	<RequestHeader>
0236	<ProtocolVersion>
0237	<ProtocolVersionMajor type="Integer" value="1"/>
0238	<ProtocolVersionMinor type="Integer" value="0"/>
0239	</ProtocolVersion>
0240	<BatchCount type="Integer" value="1"/>
0241	</RequestHeader>
0242	<BatchItem>
0243	<Operation type="Enumeration" value="GetAttributes"/>
0244	<RequestPayload>
0245	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0246	<AttributeName type="TextString" value="Archive Date"/>
0247	</RequestPayload>

0248	</BatchItem>
0249	</RequestMessage>
0250	<ResponseMessage>
0251	<ResponseHeader>
0252	<ProtocolVersion>
0253	<ProtocolVersionMajor type="Integer" value="1"/>
0254	<ProtocolVersionMinor type="Integer" value="0"/>
0255	</ProtocolVersion>
0256	<TimeStamp type="DateTime" value="2010-02-12T09:30:20+00:00"/>
0257	<BatchCount type="Integer" value="1"/>
0258	</ResponseHeader>
0259	<BatchItem>
0260	<Operation type="Enumeration" value="GetAttributes"/>
0261	<ResultStatus type="Enumeration" value="Success"/>
0262	<ResponsePayload>
0263	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0264	<Attribute>
0265	<AttributeName type="TextString" value="Archive Date"/>
0266	<AttributeValue type="DateTime" value="2010-02-
	12T09:30:18+00:00"/>
0267	</Attribute>
0268	</ResponsePayload>
0269	</BatchItem>
0270	</ResponseMessage>
	# TIME 7
0271	<RequestMessage>
0272	<RequestHeader>
0273	<ProtocolVersion>
0274	<ProtocolVersionMajor type="Integer" value="1"/>
0275	<ProtocolVersionMinor type="Integer" value="0"/>
0276	</ProtocolVersion>
0277	<BatchCount type="Integer" value="1"/>
0278	</RequestHeader>
0279	<BatchItem>
0280	<Operation type="Enumeration" value="Locate"/>
0281	<RequestPayload>
0282	<Attribute>
0283	<AttributeName type="TextString" value="Object Type"/>
0284	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0285	</Attribute>
0286	<Attribute>
0287	<AttributeName type="TextString" value="Name"/>
0288	<AttributeValue>
0289	<NameValue type="TextString" value="archiveKey"/>
0290	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0291	</AttributeValue>
0292	</Attribute>
0293	</RequestPayload>
0294	</BatchItem>
0295	</RequestMessage>
0296	<ResponseMessage>
0297	<ResponseHeader>
0298	<ProtocolVersion>
0299	<ProtocolVersionMajor type="Integer" value="1"/>

0300	<ProtocolVersionMinor type="Integer" value="0"/>
0301	</ProtocolVersion>
0302	<TimeStamp type="DateTime" value="2010-02-12T09:30:20+00:00"/>
0303	<BatchCount type="Integer" value="1"/>
0304	</ResponseHeader>
0305	<BatchItem>
0306	<Operation type="Enumeration" value="Locate"/>
0307	<ResultStatus type="Enumeration" value="Success"/>
0308	<ResponsePayload>
0309	</ResponsePayload>
0310	</BatchItem>
0311	</ResponseMessage>
# TIME 8	
0312	<RequestMessage>
0313	<RequestHeader>
0314	<ProtocolVersion>
0315	<ProtocolVersionMajor type="Integer" value="1"/>
0316	<ProtocolVersionMinor type="Integer" value="0"/>
0317	</ProtocolVersion>
0318	<BatchCount type="Integer" value="1"/>
0319	</RequestHeader>
0320	<BatchItem>
0321	<Operation type="Enumeration" value="Locate"/>
0322	<RequestPayload>
0323	<StorageStatusMask type="Integer" value="ArchivalStorage OnLineStorage"/>
0324	<Attribute>
0325	<AttributeName type="TextString" value="Object Type"/>
0326	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0327	</Attribute>
0328	<Attribute>
0329	<AttributeName type="TextString" value="Name"/>
0330	<AttributeValue>
0331	<NameValue type="TextString" value="archiveKey"/>
0332	<NameType type="Enumeration" value="UninterpretedTextString"/>
0333	</AttributeValue>
0334	</Attribute>
0335	</RequestPayload>
0336	</BatchItem>
0337	</RequestMessage>
0338	<ResponseMessage>
0339	<ResponseHeader>
0340	<ProtocolVersion>
0341	<ProtocolVersionMajor type="Integer" value="1"/>
0342	<ProtocolVersionMinor type="Integer" value="0"/>
0343	</ProtocolVersion>
0344	<TimeStamp type="DateTime" value="2010-02-12T09:30:20+00:00"/>
0345	<BatchCount type="Integer" value="1"/>
0346	</ResponseHeader>
0347	<BatchItem>
0348	<Operation type="Enumeration" value="Locate"/>
0349	<ResultStatus type="Enumeration" value="Success"/>
0350	<ResponsePayload>
0351	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0352	</ResponsePayload>

0353	</BatchItem>
0354	</ResponseMessage>
# TIME 9	
0355	<RequestMessage>
0356	<RequestHeader>
0357	<ProtocolVersion>
0358	<ProtocolVersionMajor type="Integer" value="1"/>
0359	<ProtocolVersionMinor type="Integer" value="0"/>
0360	</ProtocolVersion>
0361	<AsynchronousIndicator type="Boolean" value="true"/>
0362	<BatchCount type="Integer" value="1"/>
0363	</RequestHeader>
0364	<BatchItem>
0365	<Operation type="Enumeration" value="Recover"/>
0366	<RequestPayload>
0367	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0368	</RequestPayload>
0369	</BatchItem>
0370	</RequestMessage>
0371	<ResponseMessage>
0372	<ResponseHeader>
0373	<ProtocolVersion>
0374	<ProtocolVersionMajor type="Integer" value="1"/>
0375	<ProtocolVersionMinor type="Integer" value="0"/>
0376	</ProtocolVersion>
0377	<TimeStamp type="DateTime" value="2010-02-12T09:30:20+00:00"/>
0378	<BatchCount type="Integer" value="1"/>
0379	</ResponseHeader>
0380	<BatchItem>
0381	<Operation type="Enumeration" value="Recover"/>
0382	<ResultStatus type="Enumeration" value="OperationPending"/>
0383	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0384	</BatchItem>
0385	</ResponseMessage>
# TIME 10	
0386	<RequestMessage>
0387	<RequestHeader>
0388	<ProtocolVersion>
0389	<ProtocolVersionMajor type="Integer" value="1"/>
0390	<ProtocolVersionMinor type="Integer" value="0"/>
0391	</ProtocolVersion>
0392	<BatchCount type="Integer" value="1"/>
0393	</RequestHeader>
0394	<BatchItem>
0395	<Operation type="Enumeration" value="Poll"/>
0396	<RequestPayload>
0397	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0398	</RequestPayload>
0399	</BatchItem>
0400	</RequestMessage>
0401	<ResponseMessage>
0402	<ResponseHeader>
0403	<ProtocolVersion>

0404	<ProtocolVersionMajor type="Integer" value="1"/>
0405	<ProtocolVersionMinor type="Integer" value="0"/>
0406	</ProtocolVersion>
0407	<TimeStamp type="DateTime" value="2010-02-12T09:30:27+00:00"/>
0408	<BatchCount type="Integer" value="1"/>
0409	</ResponseHeader>
0410	<BatchItem>
0411	<Operation type="Enumeration" value="Recover"/>
0412	<ResultStatus type="Enumeration" value="Success"/>
0413	<ResponsePayload>
0414	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0415	</ResponsePayload>
0416	</BatchItem>
0417	</ResponseMessage>
# TIME 11	
0418	<RequestMessage>
0419	<RequestHeader>
0420	<ProtocolVersion>
0421	<ProtocolVersionMajor type="Integer" value="1"/>
0422	<ProtocolVersionMinor type="Integer" value="0"/>
0423	</ProtocolVersion>
0424	<BatchCount type="Integer" value="1"/>
0425	</RequestHeader>
0426	<BatchItem>
0427	<Operation type="Enumeration" value="Get"/>
0428	<RequestPayload>
0429	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0430	</RequestPayload>
0431	</BatchItem>
0432	</RequestMessage>
0433	<ResponseMessage>
0434	<ResponseHeader>
0435	<ProtocolVersion>
0436	<ProtocolVersionMajor type="Integer" value="1"/>
0437	<ProtocolVersionMinor type="Integer" value="0"/>
0438	</ProtocolVersion>
0439	<TimeStamp type="DateTime" value="2010-02-12T09:30:27+00:00"/>
0440	<BatchCount type="Integer" value="1"/>
0441	</ResponseHeader>
0442	<BatchItem>
0443	<Operation type="Enumeration" value="Get"/>
0444	<ResultStatus type="Enumeration" value="Success"/>
0445	<ResponsePayload>
0446	<ObjectType type="Enumeration" value="SymmetricKey"/>
0447	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0448	<SymmetricKey>
0449	<KeyBlock>
0450	<KeyFormatType type="Enumeration" value="Raw"/>
0451	<KeyValue>
0452	<KeyMaterial type="ByteString"
	value="c3200b1291ba648db9089ded3073de74"/>
0453	</KeyValue>
0454	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0455	<CryptographicLength type="Integer" value="128"/>

0456	</KeyBlock>
0457	</SymmetricKey>
0458	</ResponsePayload>
0459	</BatchItem>
0460	</ResponseMessage>
# TIME 12	
0461	<RequestMessage>
0462	<RequestHeader>
0463	<ProtocolVersion>
0464	<ProtocolVersionMajor type="Integer" value="1"/>
0465	<ProtocolVersionMinor type="Integer" value="0"/>
0466	</ProtocolVersion>
0467	<BatchCount type="Integer" value="1"/>
0468	</RequestHeader>
0469	<BatchItem>
0470	<Operation type="Enumeration" value="Destroy"/>
0471	<RequestPayload>
0472	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0473	</RequestPayload>
0474	</BatchItem>
0475	</RequestMessage>
0476	<ResponseMessage>
0477	<ResponseHeader>
0478	<ProtocolVersion>
0479	<ProtocolVersionMajor type="Integer" value="1"/>
0480	<ProtocolVersionMinor type="Integer" value="0"/>
0481	</ProtocolVersion>
0482	<TimeStamp type="DateTime" value="2010-02-12T09:30:28+00:00"/>
0483	<BatchCount type="Integer" value="1"/>
0484	</ResponseHeader>
0485	<BatchItem>
0486	<Operation type="Enumeration" value="Destroy"/>
0487	<ResultStatus type="Enumeration" value="Success"/>
0488	<ResponsePayload>
0489	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0490	</ResponsePayload>
0491	</BatchItem>
0492	</ResponseMessage>

179

180 2.1.20 TC-111-10 - Credential, Operation Policy, Destroy Date

181 Pass a Credential object of type Username and Password in the message header in all requests
182 for identification purposes (how the Credential object is used is defined in [KMIP-Spec]). Create
183 a symmetric key and set the Operation Policy Name attribute to 'default'. Using another
184 Username and Password Credential, attempt to perform a Get operation batched with a Get
185 Attribute List on the created symmetric key - according to the Default Operation Policy, both
186 these request SHALL fail, and with the Batch Error Continuation Option set to 'Continue', the
187 client SHALL also receive both response payloads. Using the initially used Credential, destroy the
188 object and get the Destroy Date attribute. The message exchanges in this test case are based on
189 a certain server policy (e.g. handling of Credentials) that in some aspects differs from the policy

190 assumed in earlier test cases (e.g. in this test case, the Destroy Date is retained). The message
191 exchanges shown in this test case assume that both Credentials used in this example are for
192 valid users of the server.

```
# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="0"/>
0006     </ProtocolVersion>
0007     <Authentication>
0008       <Credential>
0009         <CredentialType type="Enumeration"
value="UsernameAndPassword"/>
0010         <CredentialValue>
0011           <Username type="TextString" value="Fred"/>
0012           <Password type="TextString" value="password1"/>
0013         </CredentialValue>
0014       </Credential>
0015     </Authentication>
0016     <BatchCount type="Integer" value="1"/>
0017   </RequestHeader>
0018   <BatchItem>
0019     <Operation type="Enumeration" value="Create"/>
0020     <RequestPayload>
0021       <ObjectType type="Enumeration" value="SymmetricKey"/>
0022       <TemplateAttribute>
0023         <Attribute>
0024           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0025           <AttributeValue type="Enumeration" value="AES"/>
0026         </Attribute>
0027         <Attribute>
0028           <AttributeName type="TextString" value="Cryptographic
Length"/>
0029           <AttributeValue type="Integer" value="128"/>
0030         </Attribute>
0031         <Attribute>
0032           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0033           <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0034         </Attribute>
0035         <Attribute>
0036           <AttributeName type="TextString" value="Name"/>
0037           <AttributeValue>
0038             <NameValue type="TextString" value="PolicyKey"/>
0039             <NameType type="Enumeration"
value="UninterpretedTextString"/>
0040           </AttributeValue>
0041         </Attribute>
0042         <Attribute>
0043           <AttributeName type="TextString" value="Operation Policy
Name"/>
0044           <AttributeValue type="TextString" value="default"/>
0045         </Attribute>
```


0046	<Attribute>
0047	<AttributeName type="TextString" value="Cryptographic
	Parameters"/>
0048	<AttributeValue>
0049	<BlockCipherMode type="Enumeration" value="CBC"/>
0050	<PaddingMethod type="Enumeration" value="PKCS5"/>
0051	<HashingAlgorithm type="Enumeration" value="SHA_1"/>
0052	</AttributeValue>
0053	</Attribute>
0054	</TemplateAttribute>
0055	</RequestPayload>
0056	</BatchItem>
0057	</RequestMessage>
0058	<ResponseMessage>
0059	<ResponseHeader>
0060	<ProtocolVersion>
0061	<ProtocolVersionMajor type="Integer" value="1"/>
0062	<ProtocolVersionMinor type="Integer" value="0"/>
0063	</ProtocolVersion>
0064	<TimeStamp type="DateTime" value="2010-03-16T13:44:43+00:00"/>
0065	<BatchCount type="Integer" value="1"/>
0066	</ResponseHeader>
0067	<BatchItem>
0068	<Operation type="Enumeration" value="Create"/>
0069	<ResultStatus type="Enumeration" value="Success"/>
0070	<ResponsePayload>
0071	<ObjectType type="Enumeration" value="SymmetricKey"/>
0072	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0073	</ResponsePayload>
0074	</BatchItem>
0075	</ResponseMessage>
	# TIME 1
0076	<RequestMessage>
0077	<RequestHeader>
0078	<ProtocolVersion>
0079	<ProtocolVersionMajor type="Integer" value="1"/>
0080	<ProtocolVersionMinor type="Integer" value="0"/>
0081	</ProtocolVersion>
0082	<Authentication>
0083	<Credential>
0084	<CredentialType type="Enumeration"
	value="UsernameAndPassword"/>
0085	<CredentialValue>
0086	<Username type="TextString" value="Fred"/>
0087	<Password type="TextString" value="password1"/>
0088	</CredentialValue>
0089	</Credential>
0090	</Authentication>
0091	<BatchCount type="Integer" value="2"/>
0092	</RequestHeader>
0093	<BatchItem>
0094	<Operation type="Enumeration" value="GetAttributes"/>
0095	<UniqueBatchItemID type="ByteString" value="4cbb6751574c4da8"/>
0096	<RequestPayload>
0097	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0098	<AttributeName type="TextString" value="Operation Policy Name"/>
0099	</RequestPayload>
0100	</BatchItem>
0101	<BatchItem>
0102	<Operation type="Enumeration" value="Get"/>
0103	<UniqueBatchItemID type="ByteString" value="0ea05ee703da997b"/>
0104	<RequestPayload>
0105	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0106	</RequestPayload>
0107	</BatchItem>
0108	</RequestMessage>
0109	<ResponseMessage>
0110	<ResponseHeader>
0111	<ProtocolVersion>
0112	<ProtocolVersionMajor type="Integer" value="1"/>
0113	<ProtocolVersionMinor type="Integer" value="0"/>
0114	</ProtocolVersion>
0115	<TimeStamp type="DateTime" value="2010-03-16T13:44:44+00:00"/>
0116	<BatchCount type="Integer" value="2"/>
0117	</ResponseHeader>
0118	<BatchItem>
0119	<Operation type="Enumeration" value="GetAttributes"/>
0120	<UniqueBatchItemID type="ByteString" value="4cbb6751574c4da8"/>
0121	<ResultStatus type="Enumeration" value="Success"/>
0122	<ResponsePayload>
0123	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Operation Policy Name"/>
0126	<AttributeValue type="TextString" value="default"/>
0127	</Attribute>
0128	</ResponsePayload>
0129	</BatchItem>
0130	<BatchItem>
0131	<Operation type="Enumeration" value="Get"/>
0132	<UniqueBatchItemID type="ByteString" value="0ea05ee703da997b"/>
0133	<ResultStatus type="Enumeration" value="Success"/>
0134	<ResponsePayload>
0135	<ObjectType type="Enumeration" value="SymmetricKey"/>
0136	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0137	<SymmetricKey>
0138	<KeyBlock>
0139	<KeyFormatType type="Enumeration" value="Raw"/>
0140	<KeyValue>
0141	<KeyMaterial type="ByteString" value="c520fca4e681f7bffb3523d71427d594"/>
0142	</KeyValue>
0143	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0144	<CryptographicLength type="Integer" value="128"/>
0145	</KeyBlock>
0146	</SymmetricKey>
0147	</ResponsePayload>
0148	</BatchItem>

0149	</ResponseMessage>
	# TIME 2
0150	<RequestMessage>
0151	<RequestHeader>
0152	<ProtocolVersion>
0153	<ProtocolVersionMajor type="Integer" value="1"/>
0154	<ProtocolVersionMinor type="Integer" value="0"/>
0155	</ProtocolVersion>
0156	<Authentication>
0157	<Credential>
0158	<CredentialType type="Enumeration"
	value="UsernameAndPassword"/>
0159	<CredentialValue>
0160	<Username type="TextString" value="Barney"/>
0161	<Password type="TextString" value="secret2"/>
0162	</CredentialValue>
0163	</Credential>
0164	</Authentication>
0165	<BatchErrorContinuationOption type="Enumeration"
	value="Continue"/>
0166	<BatchOrderOption type="Boolean" value="true"/>
0167	<BatchCount type="Integer" value="2"/>
0168	</RequestHeader>
0169	<BatchItem>
0170	<Operation type="Enumeration" value="Get"/>
0171	<UniqueBatchItemID type="ByteString" value="e3e72d5a352687d8"/>
0172	<RequestPayload>
0173	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0174	</RequestPayload>
0175	</BatchItem>
0176	<BatchItem>
0177	<Operation type="Enumeration" value="GetAttributeList"/>
0178	<UniqueBatchItemID type="ByteString" value="a9ald60b0c62ecaf"/>
0179	<RequestPayload>
0180	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0181	</RequestPayload>
0182	</BatchItem>
0183	</RequestMessage>
0184	<ResponseMessage>
0185	<ResponseHeader>
0186	<ProtocolVersion>
0187	<ProtocolVersionMajor type="Integer" value="1"/>
0188	<ProtocolVersionMinor type="Integer" value="0"/>
0189	</ProtocolVersion>
0190	<TimeStamp type="DateTime" value="2010-03-16T13:44:45+00:00"/>
0191	<BatchCount type="Integer" value="2"/>
0192	</ResponseHeader>
0193	<BatchItem>
0194	<Operation type="Enumeration" value="Get"/>
0195	<UniqueBatchItemID type="ByteString" value="e3e72d5a352687d8"/>
0196	<ResultStatus type="Enumeration" value="OperationFailed"/>
0197	<ResultReason type="Enumeration" value="PermissionDenied"/>
0198	<ResultMessage type="TextString" value="Access denied"/>
0199	</BatchItem>
0200	<BatchItem>

0201	<Operation type="Enumeration" value="GetAttributeList"/>
0202	<UniqueBatchItemID type="ByteString" value="a9ald60b0c62ecaf"/>
0203	<ResultStatus type="Enumeration" value="OperationFailed"/>
0204	<ResultReason type="Enumeration" value="PermissionDenied"/>
0205	<ResultMessage type="TextString" value="Access denied"/>
0206	</BatchItem>
0207	</ResponseMessage>
# TIME 3	
0208	<RequestMessage>
0209	<RequestHeader>
0210	<ProtocolVersion>
0211	<ProtocolVersionMajor type="Integer" value="1"/>
0212	<ProtocolVersionMinor type="Integer" value="0"/>
0213	</ProtocolVersion>
0214	<Authentication>
0215	<Credential>
0216	<CredentialType type="Enumeration" value="UsernameAndPassword"/>
0217	<CredentialValue>
0218	<Username type="TextString" value="Fred"/>
0219	<Password type="TextString" value="password1"/>
0220	</CredentialValue>
0221	</Credential>
0222	</Authentication>
0223	<BatchCount type="Integer" value="1"/>
0224	</RequestHeader>
0225	<BatchItem>
0226	<Operation type="Enumeration" value="Destroy"/>
0227	<RequestPayload>
0228	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0229	</RequestPayload>
0230	</BatchItem>
0231	</RequestMessage>
0232	<ResponseMessage>
0233	<ResponseHeader>
0234	<ProtocolVersion>
0235	<ProtocolVersionMajor type="Integer" value="1"/>
0236	<ProtocolVersionMinor type="Integer" value="0"/>
0237	</ProtocolVersion>
0238	<TimeStamp type="DateTime" value="2010-03-16T13:44:45+00:00"/>
0239	<BatchCount type="Integer" value="1"/>
0240	</ResponseHeader>
0241	<BatchItem>
0242	<Operation type="Enumeration" value="Destroy"/>
0243	<ResultStatus type="Enumeration" value="Success"/>
0244	<ResponsePayload>
0245	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0246	</ResponsePayload>
0247	</BatchItem>
0248	</ResponseMessage>
# TIME 4	
0249	<RequestMessage>
0250	<RequestHeader>
0251	<ProtocolVersion>

0252	<ProtocolVersionMajor type="Integer" value="1"/>
0253	<ProtocolVersionMinor type="Integer" value="0"/>
0254	</ProtocolVersion>
0255	<Authentication>
0256	<Credential>
0257	<CredentialType type="Enumeration"
	value="UsernameAndPassword"/>
0258	<CredentialValue>
0259	<Username type="TextString" value="Fred"/>
0260	<Password type="TextString" value="password1"/>
0261	</CredentialValue>
0262	</Credential>
0263	</Authentication>
0264	<BatchCount type="Integer" value="1"/>
0265	</RequestHeader>
0266	<BatchItem>
0267	<Operation type="Enumeration" value="GetAttributes"/>
0268	<RequestPayload>
0269	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0270	<AttributeName type="TextString" value="Destroy Date"/>
0271	</RequestPayload>
0272	</BatchItem>
0273	</RequestMessage>
0274	<ResponseMessage>
0275	<ResponseHeader>
0276	<ProtocolVersion>
0277	<ProtocolVersionMajor type="Integer" value="1"/>
0278	<ProtocolVersionMinor type="Integer" value="0"/>
0279	</ProtocolVersion>
0280	<TimeStamp type="DateTime" value="2010-03-16T13:44:46+00:00"/>
0281	<BatchCount type="Integer" value="1"/>
0282	</ResponseHeader>
0283	<BatchItem>
0284	<Operation type="Enumeration" value="GetAttributes"/>
0285	<ResultStatus type="Enumeration" value="Success"/>
0286	<ResponsePayload>
0287	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0288	<Attribute>
0289	<AttributeName type="TextString" value="Destroy Date"/>
0290	<AttributeValue type="DateTime" value="2010-03-
	16T13:44:45+00:00"/>
0291	</Attribute>
0292	</ResponsePayload>
0293	</BatchItem>
0294	</ResponseMessage>

193

194 2.1.21 TC-121-10 - Query, Maximum Response Size

195 Perform a Query operation, querying the Operations and Objects supported by the server, with
196 a restriction on the Maximum Response Size set in the request header. Since the resulting Query
197 response is too big, an error is returned. Increase the Maximum Response Size, resubmit the
198 Query request, and get a successful response.

0001	# TIME 0
0002	<RequestMessage>
0003	<RequestHeader>
0004	<ProtocolVersion>
0005	<ProtocolVersionMajor type="Integer" value="1"/>
0006	<ProtocolVersionMinor type="Integer" value="0"/>
0007	</ProtocolVersion>
0008	<MaximumResponseSize type="Integer" value="256"/>
0009	<BatchCount type="Integer" value="1"/>
0010	</RequestHeader>
0011	<BatchItem>
0012	<Operation type="Enumeration" value="Query"/>
0013	<RequestPayload>
0014	<QueryFunction type="Enumeration" value="QueryOperations"/>
0015	<QueryFunction type="Enumeration" value="QueryObjects"/>
0016	</RequestPayload>
0017	</BatchItem>
0018	</RequestMessage>
0019	<ResponseMessage>
0020	<ResponseHeader>
0021	<ProtocolVersion>
0022	<ProtocolVersionMajor type="Integer" value="1"/>
0023	<ProtocolVersionMinor type="Integer" value="0"/>
0024	</ProtocolVersion>
0025	<TimeStamp type="DateTime" value="2010-02-15T09:49:30+00:00"/>
0026	<BatchCount type="Integer" value="1"/>
0027	</ResponseHeader>
0028	<BatchItem>
0029	<Operation type="Enumeration" value="Query"/>
0030	<ResultStatus type="Enumeration" value="OperationFailed"/>
0031	<ResultReason type="Enumeration" value="ResponseTooLarge"/>
0032	<ResultMessage type="TextString" value="Response size: 568, Maximum Response Size indicated in request: 256"/>
0033	</BatchItem>
0034	</ResponseMessage>
0035	# TIME 1
0036	<RequestMessage>
0037	<RequestHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="0"/>
0041	</ProtocolVersion>
0042	<MaximumResponseSize type="Integer" value="2048"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</RequestHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Query"/>
0047	<RequestPayload>
0048	<QueryFunction type="Enumeration" value="QueryOperations"/>
0049	<QueryFunction type="Enumeration" value="QueryObjects"/>
0050	</RequestPayload>
0051	</BatchItem>
0052	</RequestMessage>
0053	<ResponseMessage>
	<ResponseHeader>
	<ProtocolVersion>

0054	<ProtocolVersionMajor type="Integer" value="1"/>
0055	<ProtocolVersionMinor type="Integer" value="0"/>
0056	</ProtocolVersion>
0057	<TimeStamp type="DateTime" value="2010-02-15T09:49:30+00:00"/>
0058	<BatchCount type="Integer" value="1"/>
0059	</ResponseHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="Query"/>
0062	<ResultStatus type="Enumeration" value="Success"/>
0063	<ResponsePayload>
0064	<Operation type="Enumeration" value="Create"/>
0065	<Operation type="Enumeration" value="CreateKeyPair"/>
0066	<Operation type="Enumeration" value="Register"/>
0067	<Operation type="Enumeration" value="ReKey"/>
0068	<Operation type="Enumeration" value="Locate"/>
0069	<Operation type="Enumeration" value="Check"/>
0070	<Operation type="Enumeration" value="Get"/>
0071	<Operation type="Enumeration" value="GetAttributes"/>
0072	<Operation type="Enumeration" value="GetAttributeList"/>
0073	<Operation type="Enumeration" value="AddAttribute"/>
0074	<Operation type="Enumeration" value="ModifyAttribute"/>
0075	<Operation type="Enumeration" value="DeleteAttribute"/>
0076	<Operation type="Enumeration" value="ObtainLease"/>
0077	<Operation type="Enumeration" value="GetUsageAllocation"/>
0078	<Operation type="Enumeration" value="Activate"/>
0079	<Operation type="Enumeration" value="Revoke"/>
0080	<Operation type="Enumeration" value="Destroy"/>
0081	<Operation type="Enumeration" value="Archive"/>
0082	<Operation type="Enumeration" value="Recover"/>
0083	<Operation type="Enumeration" value="Query"/>
0084	<Operation type="Enumeration" value="Cancel"/>
0085	<Operation type="Enumeration" value="Poll"/>
0086	<ObjectType type="Enumeration" value="Certificate"/>
0087	<ObjectType type="Enumeration" value="SymmetricKey"/>
0088	<ObjectType type="Enumeration" value="PublicKey"/>
0089	<ObjectType type="Enumeration" value="PrivateKey"/>
0090	<ObjectType type="Enumeration" value="Template"/>
0091	</ResponsePayload>
0092	</BatchItem>
0093	</ResponseMessage>

199

200 2.1.22 TC-131-10 - Register an Asymmetric Key Pair in PKCS1 Format

201 Register a private key in the PKCS_1 key format, then register the corresponding public key, also
202 in PKCS_1 format, with the Link attribute pointing to the previously registered private key.
203 Thereafter add the Link attribute to the private key, and perform Locate operations to find the
204 public and private keys using the Link attribute. Get both the private and public keys in PKCS_1
205 key format, then destroy both the private and the public key.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>

```
0005     <ProtocolVersionMinor type="Integer" value="0"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008     </RequestHeader>
0009     <BatchItem>
0010         <Operation type="Enumeration" value="Register"/>
0011         <RequestPayload>
0012             <ObjectType type="Enumeration" value="PrivateKey"/>
0013             <TemplateAttribute>
0014                 <Attribute>
0015                     <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0016                     <AttributeValue type="Integer" value="Sign"/>
0017                 </Attribute>
0018                 <Attribute>
0019                     <AttributeName type="TextString" value="x-ID"/>
0020                     <AttributeValue type="TextString" value="TC-131-10-
prikey1"/>
0021                 </Attribute>
0022             </TemplateAttribute>
0023             <PrivateKey>
0024                 <KeyBlock>
0025                     <KeyFormatType type="Enumeration" value="PKCS_1"/>
0026                     <KeyValue>
0027                         <KeyMaterial type="ByteString"
value="308204a50201000282010100ab7f161c0042496ccd6c6d4dad9199734353
57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483
46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa
2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650
89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c
795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f
91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281
5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050
203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a
7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f
a74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b
2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0
e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a
a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e
3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78
965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8
c3cdc2464744a793713dafb9f1dbc799ff96423fecdc3ba794286bce920f4b5c183f
99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967
4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c
ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064
b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e
59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4
990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766
b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab
7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0
e94ad1ee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db
e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa
e1ebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2
7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eae9a22fd75d5b16b1a5
61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a72
6a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171
666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520
```


0028	a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d349417e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f8129c32341a8b44f"/>
0029	</KeyValue>
0030	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0031	<CryptographicLength type="Integer" value="2048"/>
0032	</KeyBlock>
0033	</PrivateKey>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="0"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Register"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0051	</ResponsePayload>
0052	</BatchItem>
0053	</ResponseMessage>
0054	# TIME 1
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="0"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="Register"/>
0065	<RequestPayload>
0066	<ObjectType type="Enumeration" value="PublicKey"/>
0067	<TemplateAttribute>
0068	<Attribute>
0069	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0070	<AttributeValue type="Integer" value="Verify"/>
0071	</Attribute>
0072	<Attribute>
0073	<AttributeName type="TextString" value="Link"/>
0074	<AttributeValue type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0075	</Attribute>
0076	</Attribute>

0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-131-10- pubkey1"/>
0080	</Attribute>
0081	</TemplateAttribute>
0082	<PublicKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString" value="3082010a0282010100ab7f161c0042496ccd6c6d4dadb9199734353577760 03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b 8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89 b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981 35b1c67b701675abdb7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328 abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013 da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612 a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010 001"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0089	<CryptographicLength type="Integer" value="2048"/>
0090	</KeyBlock>
0091	</PublicKey>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="0"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0109	</ResponsePayload>
0110	</BatchItem>
0111	</ResponseMessage>
0112	# TIME 2 <RequestMessage>
0113	<RequestHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="0"/>
0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="AddAttribute"/>

0122	<RequestPayload>
0123	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Link"/>
0126	<AttributeValue>
0127	<LinkType type="Enumeration" value="PublicKeyLink"/>
0128	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0129	</AttributeValue>
0130	</Attribute>
0131	</RequestPayload>
0132	</BatchItem>
0133	</RequestMessage>
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="0"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="AddAttribute"/>
0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0148	<Attribute>
0149	<AttributeName type="TextString" value="Link"/>
0150	<AttributeValue>
0151	<LinkType type="Enumeration" value="PublicKeyLink"/>
0152	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0153	</AttributeValue>
0154	</Attribute>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
	# TIME 3
0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="0"/>
0163	</ProtocolVersion>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Locate"/>
0168	<RequestPayload>
0169	<Attribute>
0170	<AttributeName type="TextString" value="Object Type"/>
0171	<AttributeValue type="Enumeration" value="PublicKey"/>
0172	</Attribute>
0173	<Attribute>

0174	<AttributeName type="TextString" value="Link"/>
0175	<AttributeValue>
0176	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0177	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0178	</AttributeValue>
0179	</Attribute>
0180	</RequestPayload>
0181	</BatchItem>
0182	</RequestMessage>
0183	<ResponseMessage>
0184	<ResponseHeader>
0185	<ProtocolVersion>
0186	<ProtocolVersionMajor type="Integer" value="1"/>
0187	<ProtocolVersionMinor type="Integer" value="0"/>
0188	</ProtocolVersion>
0189	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0190	<BatchCount type="Integer" value="1"/>
0191	</ResponseHeader>
0192	<BatchItem>
0193	<Operation type="Enumeration" value="Locate"/>
0194	<ResultStatus type="Enumeration" value="Success"/>
0195	<ResponsePayload>
0196	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0197	</ResponsePayload>
0198	</BatchItem>
0199	</ResponseMessage>
	# TIME 4
0200	<RequestMessage>
0201	<RequestHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="0"/>
0205	</ProtocolVersion>
0206	<BatchCount type="Integer" value="1"/>
0207	</RequestHeader>
0208	<BatchItem>
0209	<Operation type="Enumeration" value="Locate"/>
0210	<RequestPayload>
0211	<Attribute>
0212	<AttributeName type="TextString" value="Object Type"/>
0213	<AttributeValue type="Enumeration" value="PrivateKey"/>
0214	</Attribute>
0215	<Attribute>
0216	<AttributeName type="TextString" value="Link"/>
0217	<AttributeValue>
0218	<LinkType type="Enumeration" value="PublicKeyLink"/>
0219	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0220	</AttributeValue>
0221	</Attribute>
0222	</RequestPayload>
0223	</BatchItem>
0224	</RequestMessage>
0225	<ResponseMessage>

0226	<ResponseHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="0"/>
0230	</ProtocolVersion>
0231	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0232	<BatchCount type="Integer" value="1"/>
0233	</ResponseHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="Locate"/>
0236	<ResultStatus type="Enumeration" value="Success"/>
0237	<ResponsePayload>
0238	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0239	</ResponsePayload>
0240	</BatchItem>
0241	</ResponseMessage>
# TIME 5	
0242	<RequestMessage>
0243	<RequestHeader>
0244	<ProtocolVersion>
0245	<ProtocolVersionMajor type="Integer" value="1"/>
0246	<ProtocolVersionMinor type="Integer" value="0"/>
0247	</ProtocolVersion>
0248	<BatchCount type="Integer" value="1"/>
0249	</RequestHeader>
0250	<BatchItem>
0251	<Operation type="Enumeration" value="Get"/>
0252	<RequestPayload>
0253	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0254	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0255	</RequestPayload>
0256	</BatchItem>
0257	</RequestMessage>
0258	<ResponseMessage>
0259	<ResponseHeader>
0260	<ProtocolVersion>
0261	<ProtocolVersionMajor type="Integer" value="1"/>
0262	<ProtocolVersionMinor type="Integer" value="0"/>
0263	</ProtocolVersion>
0264	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0265	<BatchCount type="Integer" value="1"/>
0266	</ResponseHeader>
0267	<BatchItem>
0268	<Operation type="Enumeration" value="Get"/>
0269	<ResultStatus type="Enumeration" value="Success"/>
0270	<ResponsePayload>
0271	<ObjectType type="Enumeration" value="PrivateKey"/>
0272	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0273	<PrivateKey>
0274	<KeyBlock>
0275	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0276	<KeyValue>
0277	<KeyMaterial type="ByteString"
	value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353

	57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483 46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa 2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650 89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c 795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f 91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281 5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050 203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a 7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f a74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b 2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0 e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e 3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78 965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8 c3cdc2464744a793713dafb9f1dbcb799ff96423fecdd3cba794286bce920f4b5c183f 99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967 4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064 b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e 59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4 990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766 b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab 7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0 e94adlee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa elebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2 7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eae9a922fd75d5b16b1a5 61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a72 6ald90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171 666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520 a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a 1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d34941 7e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f812 9c32341a8b44f"/>
0278	</KeyValue>
0279	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0280	<CryptographicLength type="Integer" value="2048"/>
0281	</KeyBlock>
0282	</PrivateKey>
0283	</ResponsePayload>
0284	</BatchItem>
0285	</ResponseMessage>
	# TIME 6
0286	<RequestMessage>
0287	<RequestHeader>
0288	<ProtocolVersion>
0289	<ProtocolVersionMajor type="Integer" value="1"/>
0290	<ProtocolVersionMinor type="Integer" value="0"/>
0291	</ProtocolVersion>
0292	<BatchCount type="Integer" value="1"/>
0293	</RequestHeader>
0294	<BatchItem>
0295	<Operation type="Enumeration" value="Get"/>
0296	<RequestPayload>
0297	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER 1"/>

0298	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0299	</RequestPayload>
0300	</BatchItem>
0301	</RequestMessage>
0302	<ResponseMessage>
0303	<ResponseHeader>
0304	<ProtocolVersion>
0305	<ProtocolVersionMajor type="Integer" value="1"/>
0306	<ProtocolVersionMinor type="Integer" value="0"/>
0307	</ProtocolVersion>
0308	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0309	<BatchCount type="Integer" value="1"/>
0310	</ResponseHeader>
0311	<BatchItem>
0312	<Operation type="Enumeration" value="Get"/>
0313	<ResultStatus type="Enumeration" value="Success"/>
0314	<ResponsePayload>
0315	<ObjectType type="Enumeration" value="PublicKey"/>
0316	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0317	<PublicKey>
0318	<KeyBlock>
0319	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0320	<KeyValue>
0321	<KeyMaterial type="ByteString" value="3082010a0282010100ab7f161c0042496ccd6c6d4dad9199734353577760 03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b 8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89 b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981 35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328 abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013 da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612 a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010 001"/>
0322	</KeyValue>
0323	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0324	<CryptographicLength type="Integer" value="2048"/>
0325	</KeyBlock>
0326	</PublicKey>
0327	</ResponsePayload>
0328	</BatchItem>
0329	</ResponseMessage>
	# TIME 7
0330	<RequestMessage>
0331	<RequestHeader>
0332	<ProtocolVersion>
0333	<ProtocolVersionMajor type="Integer" value="1"/>
0334	<ProtocolVersionMinor type="Integer" value="0"/>
0335	</ProtocolVersion>
0336	<BatchCount type="Integer" value="1"/>
0337	</RequestHeader>
0338	<BatchItem>
0339	<Operation type="Enumeration" value="Destroy"/>
0340	<RequestPayload>
0341	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0342	</RequestPayload>

0343	</BatchItem>
0344	</RequestMessage>
0345	<ResponseMessage>
0346	<ResponseHeader>
0347	<ProtocolVersion>
0348	<ProtocolVersionMajor type="Integer" value="1"/>
0349	<ProtocolVersionMinor type="Integer" value="0"/>
0350	</ProtocolVersion>
0351	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0352	<BatchCount type="Integer" value="1"/>
0353	</ResponseHeader>
0354	<BatchItem>
0355	<Operation type="Enumeration" value="Destroy"/>
0356	<ResultStatus type="Enumeration" value="Success"/>
0357	<ResponsePayload>
0358	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0359	</ResponsePayload>
0360	</BatchItem>
0361	</ResponseMessage>
# TIME 8	
0362	<RequestMessage>
0363	<RequestHeader>
0364	<ProtocolVersion>
0365	<ProtocolVersionMajor type="Integer" value="1"/>
0366	<ProtocolVersionMinor type="Integer" value="0"/>
0367	</ProtocolVersion>
0368	<BatchCount type="Integer" value="1"/>
0369	</RequestHeader>
0370	<BatchItem>
0371	<Operation type="Enumeration" value="Destroy"/>
0372	<RequestPayload>
0373	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0374	</RequestPayload>
0375	</BatchItem>
0376	</RequestMessage>
0377	<ResponseMessage>
0378	<ResponseHeader>
0379	<ProtocolVersion>
0380	<ProtocolVersionMajor type="Integer" value="1"/>
0381	<ProtocolVersionMinor type="Integer" value="0"/>
0382	</ProtocolVersion>
0383	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0384	<BatchCount type="Integer" value="1"/>
0385	</ResponseHeader>
0386	<BatchItem>
0387	<Operation type="Enumeration" value="Destroy"/>
0388	<ResultStatus type="Enumeration" value="Success"/>
0389	<ResponsePayload>
0390	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0391	</ResponsePayload>
0392	</BatchItem>
0393	</ResponseMessage>

2.1.23 TC-132-10 - Register an Asymmetric Key Pair and a Corresponding X509 Certificate

- 209 Register a public/private key pair in the PKCS_1 key format and a corresponding X509 certificate.
210 Add the appropriate links between the registered objects. Make sure the certificate was
211 registered and the attributes set correctly by listing and retrieving the attributes. Get the keys
212 and certificate, and finally destroy all the registered objects.

```
# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="0"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="Register"/>
0011     <RequestPayload>
0012       <ObjectType type="Enumeration" value="PublicKey"/>
0013       <TemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0016           <AttributeValue type="Integer" value="Verify"/>
0017         </Attribute>
0018         <Attribute>
0019           <AttributeName type="TextString" value="x-ID"/>
0020           <AttributeValue type="TextString" value="TC-132-10-
pubkey1"/>
0021         </Attribute>
0022       </TemplateAttribute>
0023       <PublicKey>
0024         <KeyBlock>
0025           <KeyFormatType type="Enumeration" value="PKCS_1"/>
0026           <KeyValue>
0027             <KeyMaterial type="ByteString"
value="3082010a0282010100ab7f161c0042496ccd6c6d4dadb9199734353577760
03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b
8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89
b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981
35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328
abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013
da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612
a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010
001"/>
0028             </KeyValue>
0029             <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0030             <CryptographicLength type="Integer" value="2048"/>
0031           </KeyBlock>
0032         </PublicKey>
0033       </RequestPayload>
0034     </BatchItem>
0035   </RequestMessage>
```

0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="0"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="0"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PrivateKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0068	<AttributeValue type="Integer" value="Sign"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>
0073	<LinkType type="Enumeration" value="PublicKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0075	</AttributeValue>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-132-10-
	prikey1"/>
0080	</Attribute>
0081	</TemplateAttribute>
0082	<PrivateKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString"
	value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353

	57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618fa74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0aa49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8c3cdc2464744a793713dafb9f1dbcb799ff96423fecdd3cba794286bce920f4b5c183f99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d5659674c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04cec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0e94adlee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920dbe22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aaelebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee27d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eae9a922fd75d5b16b1a561fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a726a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d349417e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f8129c32341a8b44f"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0089	<CryptographicLength type="Integer" value="2048"/>
0090	</KeyBlock>
0091	</PrivateKey>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="0"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString"

0109	value="\$UNIQUE_IDENTIFIER_1"/>
0110	</ResponsePayload>
0111	</BatchItem>
0112	</ResponseMessage>
0112	# TIME 2
0113	<RequestMessage>
0114	<RequestHeader>
0115	<ProtocolVersion>
0116	<ProtocolVersionMajor type="Integer" value="1"/>
0117	<ProtocolVersionMinor type="Integer" value="0"/>
0118	</ProtocolVersion>
0119	<BatchCount type="Integer" value="1"/>
0120	</RequestHeader>
0121	<BatchItem>
0122	<Operation type="Enumeration" value="Register"/>
0123	<RequestPayload>
0124	<ObjectType type="Enumeration" value="Certificate"/>
0125	<TemplateAttribute>
0126	<Attribute>
0127	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0128	<AttributeValue type="Integer" value="Verify Sign"/>
0129	</Attribute>
0130	<Attribute>
0131	<AttributeName type="TextString" value="Link"/>
0132	<AttributeValue type="TextString" value="Link"/>
0133	<LinkType type="Enumeration" value="PublicKeyLink"/>
0134	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0135	</Attribute>
0136	<Attribute>
0137	<AttributeName type="TextString" value="x-ID"/>
0138	<AttributeValue type="TextString" value="TC-132-10-cert1"/>
0139	</Attribute>
0140	</TemplateAttribute>
0141	</Certificate>
0142	<CertificateType type="Enumeration" value="X_509"/>
0143	<CertificateValue type="ByteString" value="30820312308201faa003020102020101300d06092a864886f70d0101050500303b310b3009060355040613025553310d300b060355040a130454455354310e300c060355040b13054f41534953310d300b060355040313044b4d4950301e170d3130313130313233353935395a170d3230313130313233353935395a303b310b3009060355040613025553310d300b060355040a130454455354310e300c060355040b13054f41534953310d300b060355040313044b4d495030820122300d06092a864886f70d01010105000382010f003082010a0282010100ab7f161c0042496ccd6c6d4dadb919973435357776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89b9bee9e60ald7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010001a321301f301d0603551d0e0416041404e57bd2c431b2e816e180a19823fac858273f6b300d06092a864886f70d01010505000382010100a876adbc6c8e0ff017216e195fea76bff61a567c9a13dc50d13fec12a4273c441547cfabcb5d61d99

0144	1e966319df72c0d41ba826a45112ff26089a2344f4d71cf7c921b4bdfaef1600d1ba
0145	aa15336057e014b8b496d4fae9e8a6c1da9aeb6cbc960cbf2fae77f587ec4bb28204
0146	5338845b88dd9aeaa53e482a36e734e4f5f03b9d0dfc4cafc6bb34ea9053e52bd609
0147	ee01e86d9b09fb51120c19834a997b09ce08d79e81311762f974bb1c8c09186c4d78
	933e0db38e905084877e147c78af52fae07192ff166d19fa94a11cc11b27ed050f7a
	27fae13b205a574c4ee00aa8bd65d0d7057c985c839ef336a441ed53a53c6b6b696f
	1bdeb5f7ea811ebb25a7f86"/>
	</Certificate>
	</RequestPayload>
	</BatchItem>
	</RequestMessage>
0148	<ResponseMessage>
0149	<ResponseHeader>
0150	<ProtocolVersion>
0151	<ProtocolVersionMajor type="Integer" value="1"/>
0152	<ProtocolVersionMinor type="Integer" value="0"/>
0153	</ProtocolVersion>
0154	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0155	<BatchCount type="Integer" value="1"/>
0156	</ResponseHeader>
0157	<BatchItem>
0158	<Operation type="Enumeration" value="Register"/>
0159	<ResultStatus type="Enumeration" value="Success"/>
0160	<ResponsePayload>
0161	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0162	</ResponsePayload>
0163	</BatchItem>
0164	</ResponseMessage>
0165	# TIME 3
0166	<RequestMessage>
0167	<RequestHeader>
0168	<ProtocolVersion>
0169	<ProtocolVersionMajor type="Integer" value="1"/>
0170	<ProtocolVersionMinor type="Integer" value="0"/>
0171	</ProtocolVersion>
0172	<BatchCount type="Integer" value="2"/>
0173	</RequestHeader>
0174	<BatchItem>
0175	<Operation type="Enumeration" value="AddAttribute"/>
0176	<UniqueBatchItemID type="ByteString" value="31f81bfb0f0492bd"/>
0177	<RequestPayload>
0178	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0179	<Attribute>
0180	<AttributeName type="TextString" value="Link"/>
0181	<AttributeValue>
0182	<LinkType type="Enumeration" value="PrivateKeyLink"/>
	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0183	</AttributeValue>
0184	</Attribute>
0185	</RequestPayload>
0186	</BatchItem>
0187	<BatchItem>
0188	<Operation type="Enumeration" value="AddAttribute"/>
0189	<UniqueBatchItemID type="ByteString" value="ba865701c7837be2"/>

0190	<RequestPayload>
0191	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0192	<Attribute>
0193	<AttributeName type="TextString" value="Link"/>
0194	<AttributeValue>
0195	<LinkType type="Enumeration" value="CertificateLink"/>
0196	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0197	</AttributeValue>
0198	</Attribute>
0199	</RequestPayload>
0200	</BatchItem>
0201	</RequestMessage>
0202	<ResponseMessage>
0203	<ResponseHeader>
0204	<ProtocolVersion>
0205	<ProtocolVersionMajor type="Integer" value="1"/>
0206	<ProtocolVersionMinor type="Integer" value="0"/>
0207	</ProtocolVersion>
0208	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0209	<BatchCount type="Integer" value="2"/>
0210	</ResponseHeader>
0211	<BatchItem>
0212	<Operation type="Enumeration" value="AddAttribute"/>
0213	<UniqueBatchItemID type="ByteString" value="31f81bfb0f0492bd"/>
0214	<ResultStatus type="Enumeration" value="Success"/>
0215	<ResponsePayload>
0216	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0217	<Attribute>
0218	<AttributeName type="TextString" value="Link"/>
0219	<AttributeValue>
0220	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0221	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0222	</AttributeValue>
0223	</Attribute>
0224	</ResponsePayload>
0225	</BatchItem>
0226	<BatchItem>
0227	<Operation type="Enumeration" value="AddAttribute"/>
0228	<UniqueBatchItemID type="ByteString" value="ba865701c7837be2"/>
0229	<ResultStatus type="Enumeration" value="Success"/>
0230	<ResponsePayload>
0231	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0232	<Attribute>
0233	<AttributeName type="TextString" value="Link"/>
0234	<AttributeIndex type="Integer" value="1"/>
0235	<AttributeValue>
0236	<LinkType type="Enumeration" value="CertificateLink"/>
0237	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0238	</AttributeValue>
0239	</Attribute>
0240	</ResponsePayload>

0241	</BatchItem>
0242	</ResponseMessage>
	# TIME 4
0243	<RequestMessage>
0244	<RequestHeader>
0245	<ProtocolVersion>
0246	<ProtocolVersionMajor type="Integer" value="1"/>
0247	<ProtocolVersionMinor type="Integer" value="0"/>
0248	</ProtocolVersion>
0249	<BatchCount type="Integer" value="1"/>
0250	</RequestHeader>
0251	<BatchItem>
0252	<Operation type="Enumeration" value="GetAttributeList"/>
0253	<RequestPayload>
0254	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0255	</RequestPayload>
0256	</BatchItem>
0257	</RequestMessage>
0258	<ResponseMessage>
0259	<ResponseHeader>
0260	<ProtocolVersion>
0261	<ProtocolVersionMajor type="Integer" value="1"/>
0262	<ProtocolVersionMinor type="Integer" value="0"/>
0263	</ProtocolVersion>
0264	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0265	<BatchCount type="Integer" value="1"/>
0266	</ResponseHeader>
0267	<BatchItem>
0268	<Operation type="Enumeration" value="GetAttributeList"/>
0269	<ResultStatus type="Enumeration" value="Success"/>
0270	<ResponsePayload>
0271	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0272	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0273	<AttributeName type="TextString" value="Certificate Issuer"/>
0274	<AttributeName type="TextString" value="Certificate Type"/>
0275	<AttributeName type="TextString" value="Certificate Subject"/>
0276	<AttributeName type="TextString" value="Certificate
	Identifier"/>
0277	<AttributeName type="TextString" value="State"/>
0278	<AttributeName type="TextString" value="Digest"/>
0279	<AttributeName type="TextString" value="Link"/>
0280	<AttributeName type="TextString" value="Lease Time"/>
0281	<AttributeName type="TextString" value="Initial Date"/>
0282	<AttributeName type="TextString" value="Unique Identifier"/>
0283	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0284	<AttributeName type="TextString" value="Object Type"/>
0285	<AttributeName type="TextString" value="Last Change Date"/>
0286	<AttributeName type="TextString" value="x-ID"/>
0287	</ResponsePayload>
0288	</BatchItem>
0289	</ResponseMessage>
	# TIME 5

0290	<RequestMessage>
0291	<RequestHeader>
0292	<ProtocolVersion>
0293	<ProtocolVersionMajor type="Integer" value="1"/>
0294	<ProtocolVersionMinor type="Integer" value="0"/>
0295	</ProtocolVersion>
0296	<BatchCount type="Integer" value="1"/>
0297	</RequestHeader>
0298	<BatchItem>
0299	<Operation type="Enumeration" value="GetAttributes"/>
0300	<RequestPayload>
0301	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0302	<AttributeName type="TextString" value="Certificate
	Identifier"/>
0303	<AttributeName type="TextString" value="Certificate Issuer"/>
0304	<AttributeName type="TextString" value="Certificate Subject"/>
0305	<AttributeName type="TextString" value="Certificate Type"/>
0306	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0307	</RequestPayload>
0308	</BatchItem>
0309	</RequestMessage>
0310	<ResponseMessage>
0311	<ResponseHeader>
0312	<ProtocolVersion>
0313	<ProtocolVersionMajor type="Integer" value="1"/>
0314	<ProtocolVersionMinor type="Integer" value="0"/>
0315	</ProtocolVersion>
0316	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0317	<BatchCount type="Integer" value="1"/>
0318	</ResponseHeader>
0319	<BatchItem>
0320	<Operation type="Enumeration" value="GetAttributes"/>
0321	<ResultStatus type="Enumeration" value="Success"/>
0322	<ResponsePayload>
0323	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0324	<Attribute>
0325	<AttributeName type="TextString" value="Certificate
	Identifier"/>
0326	<AttributeValue>
0327	<Issuer type="TextString"
	value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0328	<SerialNumber type="TextString" value="1"/>
0329	</AttributeValue>
0330	</Attribute>
0331	<Attribute>
0332	<AttributeName type="TextString" value="Certificate
	Issuer"/>
0333	<AttributeValue>
0334	<CertificateIssuerDistinguishedName type="TextString"
	value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0335	</AttributeValue>
0336	</Attribute>
0337	<Attribute>
0338	<AttributeName type="TextString" value="Certificate

0339	Subject"/>
0340	<AttributeValue>
	<CertificateSubjectDistinguishedName type="TextString"
	value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0341	</AttributeValue>
0342	</Attribute>
0343	<Attribute>
0344	<AttributeName type="TextString" value="Certificate Type"/>
0345	<AttributeValue type="Enumeration" value="X_509"/>
0346	</Attribute>
0347	<Attribute>
0348	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0349	<AttributeValue type="Integer" value="2048"/>
0350	</Attribute>
0351	</ResponsePayload>
0352	</BatchItem>
0353	</ResponseMessage>
# TIME 6	
0354	<RequestMessage>
0355	<RequestHeader>
0356	<ProtocolVersion>
0357	<ProtocolVersionMajor type="Integer" value="1"/>
0358	<ProtocolVersionMinor type="Integer" value="0"/>
0359	</ProtocolVersion>
0360	<BatchCount type="Integer" value="1"/>
0361	</RequestHeader>
0362	<BatchItem>
0363	<Operation type="Enumeration" value="Get"/>
0364	<RequestPayload>
0365	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0366	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0367	</RequestPayload>
0368	</BatchItem>
0369	</RequestMessage>
0370	<ResponseMessage>
0371	<ResponseHeader>
0372	<ProtocolVersion>
0373	<ProtocolVersionMajor type="Integer" value="1"/>
0374	<ProtocolVersionMinor type="Integer" value="0"/>
0375	</ProtocolVersion>
0376	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0377	<BatchCount type="Integer" value="1"/>
0378	</ResponseHeader>
0379	<BatchItem>
0380	<Operation type="Enumeration" value="Get"/>
0381	<ResultStatus type="Enumeration" value="Success"/>
0382	<ResponsePayload>
0383	<ObjectType type="Enumeration" value="PrivateKey"/>
0384	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0385	<PrivateKey>
0386	<KeyBlock>
0387	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0388	<KeyValue>
0389	<KeyMaterial type="ByteString"

	<pre> value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353 57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483 46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa 2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650 89f98135b1c67b701675abdbcd7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c 795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f 91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281 5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050 203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a 7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f a74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b 2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0 e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e 3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78 965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8 c3cdc2464744a793713dafb9f1dbc799ff96423fecdc3ba794286bce920f4b5c183f 99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967 4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064 b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e 59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4 990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766 b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab 7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0 e94adlee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa elebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2 7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eae9a922fd75d5b16b1a5 61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a72 6ald90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171 666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520 a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a 1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d34941 7e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f812 9c32341a8b44f"/> </pre>
0390	</KeyValue>
0391	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0392	<CryptographicLength type="Integer" value="2048"/>
0393	</KeyBlock>
0394	</PrivateKey>
0395	</ResponsePayload>
0396	</BatchItem>
0397	</ResponseMessage>
	# TIME 7
0398	<RequestMessage>
0399	<RequestHeader>
0400	<ProtocolVersion>
0401	<ProtocolVersionMajor type="Integer" value="1"/>
0402	<ProtocolVersionMinor type="Integer" value="0"/>
0403	</ProtocolVersion>
0404	<BatchCount type="Integer" value="1"/>
0405	</RequestHeader>
0406	<BatchItem>
0407	<Operation type="Enumeration" value="Get"/>
0408	<RequestPayload>
0409	<UniqueIdentifier type="TextString"

0410	value="\$UNIQUE_IDENTIFIER_0"/>
0411	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0412	</RequestPayload>
0413	</BatchItem>
0414	</RequestMessage>
0415	<ResponseMessage>
0416	<ResponseHeader>
0417	<ProtocolVersion>
0418	<ProtocolVersionMajor type="Integer" value="1"/>
0419	<ProtocolVersionMinor type="Integer" value="0"/>
0420	</ProtocolVersion>
0421	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0422	<BatchCount type="Integer" value="1"/>
0423	</ResponseHeader>
0424	<BatchItem>
0425	<Operation type="Enumeration" value="Get"/>
0426	<ResultStatus type="Enumeration" value="Success"/>
0427	<ResponsePayload>
0428	<ObjectType type="Enumeration" value="PublicKey"/>
0429	<UniqueIdentifier type="TextString"
0430	value="\$UNIQUE_IDENTIFIER_0"/>
0431	<PublicKey>
0432	<KeyBlock>
0433	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0434	<KeyMaterial type="ByteString"
0435	value="3082010a0282010100ab7f161c0042496ccd6c6d4dad9199734353577760
0436	03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b
0437	8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89
0438	b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981
0439	35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328
0440	abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013
0441	da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612
0442	a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010
0443	001"/>
0444	</KeyMaterial>
0445	</KeyBlock>
0446	</PublicKey>
0447	</ResponsePayload>
0448	</BatchItem>
0449	</ResponseMessage>
0450	# TIME 8
0451	<RequestMessage>
0452	<RequestHeader>
0453	<ProtocolVersion>
0454	<ProtocolVersionMajor type="Integer" value="1"/>
0455	<ProtocolVersionMinor type="Integer" value="0"/>
0456	</ProtocolVersion>
0457	<BatchCount type="Integer" value="1"/>
0458	</RequestHeader>
0459	<BatchItem>
0460	<Operation type="Enumeration" value="Get"/>
0461	<RequestPayload>
0462	<UniqueIdentifier type="TextString"
0463	value="\$UNIQUE_IDENTIFIER_2"/>

0454	</RequestPayload>
0455	</BatchItem>
0456	</RequestMessage>
0457	<ResponseMessage>
0458	<ResponseHeader>
0459	<ProtocolVersion>
0460	<ProtocolVersionMajor type="Integer" value="1"/>
0461	<ProtocolVersionMinor type="Integer" value="0"/>
0462	</ProtocolVersion>
0463	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0464	<BatchCount type="Integer" value="1"/>
0465	</ResponseHeader>
0466	<BatchItem>
0467	<Operation type="Enumeration" value="Get"/>
0468	<ResultStatus type="Enumeration" value="Success"/>
0469	<ResponsePayload>
0470	<ObjectType type="Enumeration" value="Certificate"/>
0471	<UniqueIdentifier type="TextString"
0472	value="\$UNIQUE_IDENTIFIER_2"/>
0473	<Certificate>
0474	<CertificateType type="Enumeration" value="X_509"/>
0475	<CertificateValue type="ByteString"
0476	value="30820312308201faa003020102020101300d06092a864886f70d010105050
0477	0303b310b3009060355040613025553310d300b060355040a130454455354310e300
0478	c060355040b13054f41534953310d300b060355040313044b4d4950301e170d31303
	13130313233353935395a170d3230313130313233353935395a303b310b300906035
	5040613025553310d300b060355040a130454455354310e300c060355040b13054f4
	1534953310d300b060355040313044b4d495030820122300d06092a864886f70d010
	10105000382010f003082010a0282010100ab7f161c0042496ccd6c6d4dad919973
	435357776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74
	648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc62
	67fa2a6f89b9bee9e60ald7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8
	b65089f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295
	353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142c
	b76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1
	c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f
	6050203010001a321301f301d0603551d0e0416041404e57bd2c431b2e816e180a19
	823fac858273f6b300d06092a864886f70d0101050500382010100a876adbc6c8e0
	ff017216e195fea76bff61a567c9a13dc50d13fec12a4273c441547cfabcb5d61d99
	1e966319df72c0d41ba826a45112ff26089a2344f4d71cf7c921b4bdfaef1600d1ba
	aa15336057e014b8b496d4fae9e8a6c1da9aeb6cbc960cbf2fae77f587ec4bb28204
	5338845b88dd9aeaa53e482a36e734e4f5f03b9d0dfc4cafc6bb34ea9053e52bd609
	ee01e86d9b09fb51120c19834a997b09ce08d79e81311762f974bb1c8c09186c4d78
	933e0db38e905084877e147c78af52fae07192ff166d19fa94a11cc11b27ed050f7a
	27fae13b205a574c4ee00aa8bd65d0d7057c985c839ef336a441ed53a53c6b6b696f
	1bdeb5f7ea811ebb25a7f86"/>
0475	</Certificate>
0476	</ResponsePayload>
0477	</BatchItem>
0478	</ResponseMessage>
0479	# TIME 9
0480	<RequestMessage>
0481	<RequestHeader>
0482	<ProtocolVersion>
0483	<ProtocolVersionMajor type="Integer" value="1"/>
0484	<ProtocolVersionMinor type="Integer" value="0"/>
	</ProtocolVersion>

0485	<BatchCount type="Integer" value="1"/>
0486	</RequestHeader>
0487	<BatchItem>
0488	<Operation type="Enumeration" value="Destroy"/>
0489	<RequestPayload>
0490	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0491	</RequestPayload>
0492	</BatchItem>
0493	</RequestMessage>
0494	<ResponseMessage>
0495	<ResponseHeader>
0496	<ProtocolVersion>
0497	<ProtocolVersionMajor type="Integer" value="1"/>
0498	<ProtocolVersionMinor type="Integer" value="0"/>
0499	</ProtocolVersion>
0500	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0501	<BatchCount type="Integer" value="1"/>
0502	</ResponseHeader>
0503	<BatchItem>
0504	<Operation type="Enumeration" value="Destroy"/>
0505	<ResultStatus type="Enumeration" value="Success"/>
0506	<ResponsePayload>
0507	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0508	</ResponsePayload>
0509	</BatchItem>
0510	</ResponseMessage>
	# TIME 10
0511	<RequestMessage>
0512	<RequestHeader>
0513	<ProtocolVersion>
0514	<ProtocolVersionMajor type="Integer" value="1"/>
0515	<ProtocolVersionMinor type="Integer" value="0"/>
0516	</ProtocolVersion>
0517	<BatchCount type="Integer" value="1"/>
0518	</RequestHeader>
0519	<BatchItem>
0520	<Operation type="Enumeration" value="Destroy"/>
0521	<RequestPayload>
0522	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0523	</RequestPayload>
0524	</BatchItem>
0525	</RequestMessage>
0526	<ResponseMessage>
0527	<ResponseHeader>
0528	<ProtocolVersion>
0529	<ProtocolVersionMajor type="Integer" value="1"/>
0530	<ProtocolVersionMinor type="Integer" value="0"/>
0531	</ProtocolVersion>
0532	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0533	<BatchCount type="Integer" value="1"/>
0534	</ResponseHeader>
0535	<BatchItem>
0536	<Operation type="Enumeration" value="Destroy"/>

0537	<ResultStatus type="Enumeration" value="Success"/>
0538	<ResponsePayload>
0539	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0540	</ResponsePayload>
0541	</BatchItem>
0542	</ResponseMessage>
# TIME 11	
0543	<RequestMessage>
0544	<RequestHeader>
0545	<ProtocolVersion>
0546	<ProtocolVersionMajor type="Integer" value="1"/>
0547	<ProtocolVersionMinor type="Integer" value="0"/>
0548	</ProtocolVersion>
0549	<BatchCount type="Integer" value="1"/>
0550	</RequestHeader>
0551	<BatchItem>
0552	<Operation type="Enumeration" value="Destroy"/>
0553	<RequestPayload>
0554	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0555	</RequestPayload>
0556	</BatchItem>
0557	</RequestMessage>
0558	<ResponseMessage>
0559	<ResponseHeader>
0560	<ProtocolVersion>
0561	<ProtocolVersionMajor type="Integer" value="1"/>
0562	<ProtocolVersionMinor type="Integer" value="0"/>
0563	</ProtocolVersion>
0564	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0565	<BatchCount type="Integer" value="1"/>
0566	</ResponseHeader>
0567	<BatchItem>
0568	<Operation type="Enumeration" value="Destroy"/>
0569	<ResultStatus type="Enumeration" value="Success"/>
0570	<ResponsePayload>
0571	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0572	</ResponsePayload>
0573	</BatchItem>
0574	</ResponseMessage>

213

214 2.1.24 TC-134-10 - Register Key Pair, Certify and Re-certify Public Key

215 Register a public/private key pair on the server. Request the server to have a certificate created
216 using the Certify operation. Retrieve the certificate and its attributes, then execute the Re-
217 certify operation to re-certify the public key. Finally, destroy all the objects.

218 The new KMIP 1.1 certificate DN attributes are retrieved as are the original (deprecated) KMIP
219 1.0 certificate DN attributes.

# TIME 0	
0001	<RequestMessage>

0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="PublicKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Verify"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-134-10-pubkey1"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<PublicKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString" value="3082010a0282010100ab7f161c0042496ccd6c6d4dadb919973435357776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f98135b1c67b701675abdbbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010001"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0030	<CryptographicLength type="Integer" value="2048"/>
0031	</KeyBlock>
0032	</PublicKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="0"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>

0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
0050	value="\$UNIQUE_IDENTIFIER_0"/>
0051	</ResponsePayload>
0052	</BatchItem>
0053	</ResponseMessage>
0054	# TIME 1
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="0"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="Register"/>
0065	<RequestPayload>
0066	<ObjectType type="Enumeration" value="PrivateKey"/>
0067	<TemplateAttribute>
0068	<Attribute>
0069	<AttributeName type="TextString" value="Cryptographic
0070	Usage Mask"/>
0071	<AttributeValue type="Integer" value="Sign"/>
0072	</Attribute>
0073	<Attribute>
0074	<AttributeName type="TextString" value="Link"/>
0075	<AttributeValue>
0076	<LinkType type="Enumeration" value="PublicKeyLink"/>
0077	<LinkedObjectIdentifier type="TextString"
0078	value="\$UNIQUE_IDENTIFIER_0"/>
0079	</AttributeValue>
0080	</Attribute>
0081	<Attribute>
0082	<AttributeName type="TextString" value="x-ID"/>
0083	<AttributeValue type="TextString" value="TC-134-10-
0084	prikey1"/>
0085	</Attribute>
0086	</TemplateAttribute>
	<PrivateKey>
	<KeyBlock>
	<KeyFormatType type="Enumeration" value="PKCS_1"/>
	<KeyValue>
	<KeyMaterial type="ByteString"
	value="308204a50201000282010100ab7f161c0042496ccd6c6d4dad9b9199734353
	57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483
	46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa
	2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650
	89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c
	795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f
	91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281
	5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050
	203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a
	7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f
	a74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b
	2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0
	e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a

	<pre> a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e 3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78 965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8 c3cdc2464744a793713dafb9f1dbc799ff96423fecdc3ba794286bce920f4b5c183f 99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967 4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064 b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e 59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4 990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766 b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab 7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0 e94adlee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa elebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2 7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eaeafa922fd75d5b16b1a5 61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a72 6ald90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171 666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520 a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a 1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d34941 7elf0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f812 9c32341a8b44f"/> </KeyValue> <CryptographicAlgorithm type="Enumeration" value="RSA"/> <CryptographicLength type="Integer" value="2048"/> </KeyBlock> </PrivateKey> </RequestPayload> </BatchItem> </RequestMessage> </pre>
0087	
0088	
0089	
0090	
0091	
0092	
0093	
0094	
0095	<pre> <ResponseMessage> <ResponseHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="0"/> </ProtocolVersion> <TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/> <BatchCount type="Integer" value="1"/> </ResponseHeader> <BatchItem> <Operation type="Enumeration" value="Register"/> <ResultStatus type="Enumeration" value="Success"/> <ResponsePayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> </ResponsePayload> </BatchItem> </ResponseMessage> </pre>
0096	
0097	
0098	
0099	
0100	
0101	
0102	
0103	
0104	
0105	
0106	
0107	
0108	
0109	
0110	
0111	
	<pre> # TIME 2 <RequestMessage> <RequestHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="0"/> </ProtocolVersion> <BatchCount type="Integer" value="1"/> </pre>
0112	
0113	
0114	
0115	
0116	
0117	
0118	

0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="AddAttribute"/>
0122	<RequestPayload>
0123	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Link"/>
0126	<AttributeValue>
0127	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0128	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0129	</AttributeValue>
0130	</Attribute>
0131	</RequestPayload>
0132	</BatchItem>
0133	</RequestMessage>
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="0"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="AddAttribute"/>
0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0148	<Attribute>
0149	<AttributeName type="TextString" value="Link"/>
0150	<AttributeValue>
0151	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0152	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0153	</AttributeValue>
0154	</Attribute>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
	# TIME 3
0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="0"/>
0163	</ProtocolVersion>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Certify"/>
0168	<RequestPayload>
0169	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0170	<CertificateRequestType type="Enumeration" value="PKCS_10"/>
0171	<CertificateRequest type="ByteString"
	value="3082028130820169020100303c310b3009060355040613025553310d300b060355040a130441434d45310d300b060355040b13044b4d4950310f300d06035504031306436c69656e7430820122300d06092a864886f70d01010105000382010f003082010a0282010100ab7f161c0042496ccd6c6d4dad919973435357776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f98135b1c67b701675abdbbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010001a000300d06092a864886f70d010105050003820101002d90f5492c3df1771df4e87e1087cb952197319a9696e2d588efda580d8d3304427b997cd921ad7c674aea413fba85fd61e6a481de9ab2e8a4ff43c02655015d3437f783fe0c781519cd08ffd3c007c7fade9632fe5659e2cac35bd6aaf3e13dc18097d996df01b66fc5e26ca109380863a209125cc0fd79533f327falcad444d89d3ff81b92a91428c469c846090fd1324846e12d01671962c332a7826152daaf486cc867185c2e27caf2f009898db07fe4b45c518192aa493d8f8c0198db67f90672ab6de05a08032941377f473d80716d85adc6182003ab34942302214eb3895f15403f2616adfd6bb5e6aa47fa38c9dfc73f4de80ddb91bdb04d21c82ba6"/>
0172	<TemplateAttribute>
0173	<Attribute>
0174	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0175	<AttributeValue type="Integer" value="Verify Sign"/>
0176	</Attribute>
0177	<Attribute>
0178	<AttributeName type="TextString" value="Name"/>
0179	<AttributeValue>
0180	<NameValue type="TextString" value="TC-134-10-certificate1"/>
0181	<NameType type="Enumeration" value="UninterpretedTextString"/>
0182	</AttributeValue>
0183	</Attribute>
0184	</TemplateAttribute>
0185	</RequestPayload>
0186	</BatchItem>
0187	</RequestMessage>
0188	<ResponseMessage>
0189	<ResponseHeader>
0190	<ProtocolVersion>
0191	<ProtocolVersionMajor type="Integer" value="1"/>
0192	<ProtocolVersionMinor type="Integer" value="0"/>
0193	</ProtocolVersion>
0194	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0195	<BatchCount type="Integer" value="1"/>
0196	</ResponseHeader>
0197	<BatchItem>
0198	<Operation type="Enumeration" value="Certify"/>
0199	<ResultStatus type="Enumeration" value="Success"/>
0200	<ResponsePayload>
0201	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0202	</ResponsePayload>

0203	</BatchItem>
0204	</ResponseMessage>
# TIME 4	
0205	<RequestMessage>
0206	<RequestHeader>
0207	<ProtocolVersion>
0208	<ProtocolVersionMajor type="Integer" value="1"/>
0209	<ProtocolVersionMinor type="Integer" value="0"/>
0210	</ProtocolVersion>
0211	<BatchCount type="Integer" value="1"/>
0212	</RequestHeader>
0213	<BatchItem>
0214	<Operation type="Enumeration" value="Get"/>
0215	<RequestPayload>
0216	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0217	</RequestPayload>
0218	</BatchItem>
0219	</RequestMessage>
0220	<ResponseMessage>
0221	<ResponseHeader>
0222	<ProtocolVersion>
0223	<ProtocolVersionMajor type="Integer" value="1"/>
0224	<ProtocolVersionMinor type="Integer" value="0"/>
0225	</ProtocolVersion>
0226	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0227	<BatchCount type="Integer" value="1"/>
0228	</ResponseHeader>
0229	<BatchItem>
0230	<Operation type="Enumeration" value="Get"/>
0231	<ResultStatus type="Enumeration" value="Success"/>
0232	<ResponsePayload>
0233	<ObjectType type="Enumeration" value="Certificate"/>
0234	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0235	<Certificate>
0236	<CertificateType type="Enumeration" value="X_509"/>
0237	<CertificateValue type="ByteString" value="30820277308201e0a0030201020209009bba23d1b6a48f97300d06092a864 886f70d01010b0500303b310b3009060355040613025553310d300b060355040a130 454455354310e300c060355040b13054f41534953310d300b060355040313044b4d4 950301e170d3133303631383038353535375a170d3134303631383038353535375a3 03c310b3009060355040613025553310d300b060355040a130441434d45310d300b0 60355040b13044b4d4950310f300d06035504031306436c69656e7430820122300d0 6092a864886f70d01010105000382010f003082010a0282010100ab7f161c0042496 ccd6c6d4dad919973435357776003acf54b7af1e440afb80b64a8755f8002cfeba6 b184540a2d66086d74648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176 b7957c422e7d03fc6267fa2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a 41100f8aa214900df8b65089f98135b1c67b701675abdbc7d5721aac9d14a7f081fc ec80b64e8a0ecc8295353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d2112 6eba8da7d0ca34142cb76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c 8d7cce8946a9ac99b1c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6f c411335d5dc7426b0f6050203010001300d06092a864886f70d01010b05000381810 0c4fe08d5bd74239648c7faabaed0978527ac01a0fd17b8a65c0d92501c4eab3f487 511062eafedc1024e74dc6bfdaae7f66d1fdda7574f6db3f03c6de83586b52c593a4 671001a0531bc43eff4849880b07924b7a9a0236d5d64d82d4d8e42dcd3a72c80728 804f9ba7f0e80c3fe3eb09cb3ed7fbfbb2167c99be513ff9db0b6"/>

0238	</Certificate>
0239	</ResponsePayload>
0240	</BatchItem>
0241	</ResponseMessage>
0242	# TIME 5 <RequestMessage>
0243	<RequestHeader>
0244	<ProtocolVersion>
0245	<ProtocolVersionMajor type="Integer" value="1"/>
0246	<ProtocolVersionMinor type="Integer" value="0"/>
0247	</ProtocolVersion>
0248	<BatchCount type="Integer" value="1"/>
0249	</RequestHeader>
0250	<BatchItem>
0251	<Operation type="Enumeration" value="GetAttributeList"/>
0252	<RequestPayload>
0253	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0254	</RequestPayload>
0255	</BatchItem>
0256	</RequestMessage>
0257	<ResponseMessage>
0258	<ResponseHeader>
0259	<ProtocolVersion>
0260	<ProtocolVersionMajor type="Integer" value="1"/>
0261	<ProtocolVersionMinor type="Integer" value="0"/>
0262	</ProtocolVersion>
0263	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0264	<BatchCount type="Integer" value="1"/>
0265	</ResponseHeader>
0266	<BatchItem>
0267	<Operation type="Enumeration" value="GetAttributeList"/>
0268	<ResultStatus type="Enumeration" value="Success"/>
0269	<ResponsePayload>
0270	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0271	<AttributeName type="TextString" value="Cryptographic Length"/>
0272	<AttributeName type="TextString" value="Certificate Issuer"/>
0273	<AttributeName type="TextString" value="Certificate Type"/>
0274	<AttributeName type="TextString" value="Certificate Subject"/>
0275	<AttributeName type="TextString" value="Certificate Identifier"/>
0276	<AttributeName type="TextString" value="State"/>
0277	<AttributeName type="TextString" value="Digest"/>
0278	<AttributeName type="TextString" value="Link"/>
0279	<AttributeName type="TextString" value="Lease Time"/>
0280	<AttributeName type="TextString" value="Initial Date"/>
0281	<AttributeName type="TextString" value="Unique Identifier"/>
0282	<AttributeName type="TextString" value="Name"/>
0283	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0284	<AttributeName type="TextString" value="Object Type"/>
0285	<AttributeName type="TextString" value="Last Change Date"/>
0286	</ResponsePayload>
0287	</BatchItem>
0288	</ResponseMessage>

	# TIME 6
0289	<RequestMessage>
0290	<RequestHeader>
0291	<ProtocolVersion>
0292	<ProtocolVersionMajor type="Integer" value="1"/>
0293	<ProtocolVersionMinor type="Integer" value="0"/>
0294	</ProtocolVersion>
0295	<BatchCount type="Integer" value="1"/>
0296	</RequestHeader>
0297	<BatchItem>
0298	<Operation type="Enumeration" value="GetAttributes"/>
0299	<RequestPayload>
0300	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0301	<AttributeName type="TextString" value="Certificate
	Identifier"/>
0302	<AttributeName type="TextString" value="Certificate Issuer"/>
0303	<AttributeName type="TextString" value="Certificate Subject"/>
0304	<AttributeName type="TextString" value="Certificate Type"/>
0305	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0306	</RequestPayload>
0307	</BatchItem>
0308	</RequestMessage>
0309	<ResponseMessage>
0310	<ResponseHeader>
0311	<ProtocolVersion>
0312	<ProtocolVersionMajor type="Integer" value="1"/>
0313	<ProtocolVersionMinor type="Integer" value="0"/>
0314	</ProtocolVersion>
0315	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0316	<BatchCount type="Integer" value="1"/>
0317	</ResponseHeader>
0318	<BatchItem>
0319	<Operation type="Enumeration" value="GetAttributes"/>
0320	<ResultStatus type="Enumeration" value="Success"/>
0321	<ResponsePayload>
0322	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0323	<Attribute>
0324	<AttributeName type="TextString" value="Certificate
	Identifier"/>
0325	<AttributeValue>
0326	<Issuer type="TextString"
	value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0327	<SerialNumber type="TextString" value="9BBA23D1B6A48F97"/>
0328	</AttributeValue>
0329	</Attribute>
0330	<Attribute>
0331	<AttributeName type="TextString" value="Certificate
	Issuer"/>
0332	<AttributeValue>
0333	<CertificateIssuerDistinguishedName type="TextString"
	value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0334	</AttributeValue>
0335	</Attribute>
0336	</ResponsePayload>

0337	<AttributeName type="TextString" value="Certificate
0338	Subject"/>
0339	<AttributeValue>
	<CertificateSubjectDistinguishedName type="TextString"
	value="CN=Client,OU=KMIP,O=ACME,C=US"/>
0340	</AttributeValue>
0341	</Attribute>
0342	<Attribute>
0343	<AttributeName type="TextString" value="Certificate Type"/>
0344	<AttributeValue type="Enumeration" value="X_509"/>
0345	</Attribute>
0346	<Attribute>
0347	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0348	<AttributeValue type="Integer" value="2048"/>
0349	</Attribute>
0350	</ResponsePayload>
0351	</BatchItem>
0352	</ResponseMessage>
	# TIME 7
0353	<RequestMessage>
0354	<RequestHeader>
0355	<ProtocolVersion>
0356	<ProtocolVersionMajor type="Integer" value="1"/>
0357	<ProtocolVersionMinor type="Integer" value="0"/>
0358	</ProtocolVersion>
0359	<BatchCount type="Integer" value="1"/>
0360	</RequestHeader>
0361	<BatchItem>
0362	<Operation type="Enumeration" value="ReCertify"/>
0363	<RequestPayload>
0364	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0365	<CertificateRequestType type="Enumeration" value="PKCS_10"/>
0366	<CertificateRequest type="ByteString"
	value="3082028130820169020100303c310b3009060355040613025553310d300b0
	60355040a130441434d45310d300b060355040b13044b4d4950310f300d060355040
	31306436c69656e7430820122300d06092a864886f70d01010105000382010f00308
	2010a0282010100ab7f161c0042496ccd6c6d4dad919973435357776003acf54b7a
	f1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b8d71812b20
	5387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89b9bee9e60a
	1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f98135b1c67b70
	1675abdbbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328abf70e1b42
	e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da809e9c1b
	7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a29a82d73a
	1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010001a000300
	d06092a864886f70d010105050003820101002d90f5492c3df1771df4e87e1087cb9
	52197319a9696e2d588efda580d8d3304427b997cd921ad7c674aea413fba85fd61e
	6a481de9ab2e8a4ff43c02655015d3437f783fe0c781519cd08ffd3c007c7fade963
	2fe5659e2cac35bd6aaf3e13dc18097d996df01b66fc5e26ca109380863a209125cc
	0fd79533f327falcad444d89d3ff81b92a91428c469c846090fd1324846e12d01671
	962c332a7826152daaf486cc867185c2e27caf2f009898db07fe4b45c518192aa493
	d8f8c0198db67f90672ab6de05a08032941377f473d80716d85adc6182003ab34942
	302214eb3895f15403f2616adfd6bb5e6aa47fa38c9dfc73f4de80ddb91bdb04d21c
	82ba6"/>
0367	<TemplateAttribute>
0368	<Attribute>

0369	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0370	<AttributeValue type="Integer" value="Verify Sign"/>
0371	</Attribute>
0372	<Attribute>
0373	<AttributeName type="TextString" value="Name"/>
0374	<AttributeValue>
0375	<NameValue type="TextString" value="TC-134-10-certificate2"/>
0376	<NameType type="Enumeration" value="UninterpretedTextString"/>
0377	</AttributeValue>
0378	</Attribute>
0379	</TemplateAttribute>
0380	</RequestPayload>
0381	</BatchItem>
0382	</RequestMessage>
0383	<ResponseMessage>
0384	<ResponseHeader>
0385	<ProtocolVersion>
0386	<ProtocolVersionMajor type="Integer" value="1"/>
0387	<ProtocolVersionMinor type="Integer" value="0"/>
0388	</ProtocolVersion>
0389	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0390	<BatchCount type="Integer" value="1"/>
0391	</ResponseHeader>
0392	<BatchItem>
0393	<Operation type="Enumeration" value="ReCertify"/>
0394	<ResultStatus type="Enumeration" value="Success"/>
0395	<ResponsePayload>
0396	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_3"/>
0397	</ResponsePayload>
0398	</BatchItem>
0399	</ResponseMessage>
# TIME 8	
0400	<RequestMessage>
0401	<RequestHeader>
0402	<ProtocolVersion>
0403	<ProtocolVersionMajor type="Integer" value="1"/>
0404	<ProtocolVersionMinor type="Integer" value="0"/>
0405	</ProtocolVersion>
0406	<BatchCount type="Integer" value="1"/>
0407	</RequestHeader>
0408	<BatchItem>
0409	<Operation type="Enumeration" value="GetAttributes"/>
0410	<RequestPayload>
0411	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0412	<AttributeName type="TextString" value="Link"/>
0413	</RequestPayload>
0414	</BatchItem>
0415	</RequestMessage>
0416	<ResponseMessage>
0417	<ResponseHeader>
0418	<ProtocolVersion>

0419	<ProtocolVersionMajor type="Integer" value="1"/>
0420	<ProtocolVersionMinor type="Integer" value="0"/>
0421	</ProtocolVersion>
0422	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0423	<BatchCount type="Integer" value="1"/>
0424	</ResponseHeader>
0425	<BatchItem>
0426	<Operation type="Enumeration" value="GetAttributes"/>
0427	<ResultStatus type="Enumeration" value="Success"/>
0428	<ResponsePayload>
0429	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0430	<Attribute>
0431	<AttributeName type="TextString" value="Link"/>
0432	<AttributeValue>
0433	<LinkType type="Enumeration" value="PublicKeyLink"/>
0434	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0435	</AttributeValue>
0436	</Attribute>
0437	</ResponsePayload>
0438	</BatchItem>
0439	</ResponseMessage>
# TIME 9	
0440	<RequestMessage>
0441	<RequestHeader>
0442	<ProtocolVersion>
0443	<ProtocolVersionMajor type="Integer" value="1"/>
0444	<ProtocolVersionMinor type="Integer" value="0"/>
0445	</ProtocolVersion>
0446	<BatchCount type="Integer" value="1"/>
0447	</RequestHeader>
0448	<BatchItem>
0449	<Operation type="Enumeration" value="GetAttributes"/>
0450	<RequestPayload>
0451	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0452	<AttributeName type="TextString" value="Link"/>
0453	</RequestPayload>
0454	</BatchItem>
0455	</RequestMessage>
0456	<ResponseMessage>
0457	<ResponseHeader>
0458	<ProtocolVersion>
0459	<ProtocolVersionMajor type="Integer" value="1"/>
0460	<ProtocolVersionMinor type="Integer" value="0"/>
0461	</ProtocolVersion>
0462	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0463	<BatchCount type="Integer" value="1"/>
0464	</ResponseHeader>
0465	<BatchItem>
0466	<Operation type="Enumeration" value="GetAttributes"/>
0467	<ResultStatus type="Enumeration" value="Success"/>
0468	<ResponsePayload>
0469	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0470	<Attribute>

0471	<AttributeName type="TextString" value="Link"/>
0472	<AttributeValue>
0473	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0474	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0475	</AttributeValue>
0476	</Attribute>
0477	<Attribute>
0478	<AttributeName type="TextString" value="Link"/>
0479	<AttributeIndex type="Integer" value="1"/>
0480	<AttributeValue>
0481	<LinkType type="Enumeration" value="CertificateLink"/>
0482	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0483	</AttributeValue>
0484	</Attribute>
0485	</ResponsePayload>
0486	</BatchItem>
0487	</ResponseMessage>
	# TIME 10
0488	<RequestMessage>
0489	<RequestHeader>
0490	<ProtocolVersion>
0491	<ProtocolVersionMajor type="Integer" value="1"/>
0492	<ProtocolVersionMinor type="Integer" value="0"/>
0493	</ProtocolVersion>
0494	<BatchCount type="Integer" value="1"/>
0495	</RequestHeader>
0496	<BatchItem>
0497	<Operation type="Enumeration" value="GetAttributes"/>
0498	<RequestPayload>
0499	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0500	<AttributeName type="TextString" value="Link"/>
0501	</RequestPayload>
0502	</BatchItem>
0503	</RequestMessage>
0504	<ResponseMessage>
0505	<ResponseHeader>
0506	<ProtocolVersion>
0507	<ProtocolVersionMajor type="Integer" value="1"/>
0508	<ProtocolVersionMinor type="Integer" value="0"/>
0509	</ProtocolVersion>
0510	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0511	<BatchCount type="Integer" value="1"/>
0512	</ResponseHeader>
0513	<BatchItem>
0514	<Operation type="Enumeration" value="GetAttributes"/>
0515	<ResultStatus type="Enumeration" value="Success"/>
0516	<ResponsePayload>
0517	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0518	<Attribute>
0519	<AttributeName type="TextString" value="Link"/>
0520	<AttributeValue>
0521	<LinkType type="Enumeration" value="PublicKeyLink"/>
0522	<LinkedObjectIdentifier type="TextString"

0523	value="\$UNIQUE_IDENTIFIER_0"/>
0524	</AttributeValue>
0525	</Attribute>
0526	<AttributeName type="TextString" value="Link"/>
0527	<AttributeIndex type="Integer" value="1"/>
0528	<AttributeValue>
0529	<LinkType type="Enumeration"
	value="ReplacementObjectLink"/>
0530	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0531	</AttributeValue>
0532	</Attribute>
0533	</ResponsePayload>
0534	</BatchItem>
0535	</ResponseMessage>
	# TIME 11
0536	<RequestMessage>
0537	<RequestHeader>
0538	<ProtocolVersion>
0539	<ProtocolVersionMajor type="Integer" value="1"/>
0540	<ProtocolVersionMinor type="Integer" value="0"/>
0541	</ProtocolVersion>
0542	<BatchCount type="Integer" value="1"/>
0543	</RequestHeader>
0544	<BatchItem>
0545	<Operation type="Enumeration" value="GetAttributes"/>
0546	<RequestPayload>
0547	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0548	<AttributeName type="TextString" value="Link"/>
0549	<AttributeName type="TextString" value="Certificate
	Identifier"/>
0550	<AttributeName type="TextString" value="Name"/>
0551	</RequestPayload>
0552	</BatchItem>
0553	</RequestMessage>
0554	<ResponseMessage>
0555	<ResponseHeader>
0556	<ProtocolVersion>
0557	<ProtocolVersionMajor type="Integer" value="1"/>
0558	<ProtocolVersionMinor type="Integer" value="0"/>
0559	</ProtocolVersion>
0560	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0561	<BatchCount type="Integer" value="1"/>
0562	</ResponseHeader>
0563	<BatchItem>
0564	<Operation type="Enumeration" value="GetAttributes"/>
0565	<ResultStatus type="Enumeration" value="Success"/>
0566	<ResponsePayload>
0567	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0568	<Attribute>
0569	<AttributeName type="TextString" value="Link"/>
0570	<AttributeValue>
0571	<LinkType type="Enumeration" value="ReplacedObjectLink"/>
0572	<LinkedObjectIdentifier type="TextString"

0573	value="\$UNIQUE_IDENTIFIER_2"/>
0574	</AttributeValue>
0575	</Attribute>
0576	<AttributeName type="TextString" value="Link"/>
0577	<AttributeIndex type="Integer" value="1"/>
0578	<AttributeValue>
0579	<LinkType type="Enumeration" value="PublicKeyLink"/>
0580	<LinkedObjectIdentifier type="TextString"
0581	value="\$UNIQUE_IDENTIFIER_0"/>
0582	</AttributeValue>
0583	</Attribute>
0584	<AttributeName type="TextString" value="Certificate
0585	Identifier"/>
0586	<AttributeValue>
0587	<Issuer type="TextString"
0588	value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0589	<SerialNumber type="TextString" value="CF77F7A23282BC12"/>
0590	</AttributeValue>
0591	</Attribute>
0592	<AttributeName type="TextString" value="Name"/>
0593	<AttributeValue>
0594	<NameValue type="TextString" value="TC-134-10-
0595	certificate1"/>
0596	<NameType type="Enumeration"
0597	value="UninterpretedTextString"/>
0598	</AttributeValue>
0599	</Attribute>
0600	<AttributeName type="TextString" value="Name"/>
0601	<AttributeIndex type="Integer" value="1"/>
0602	<AttributeValue>
0603	<NameValue type="TextString" value="TC-134-10-
0604	certificate2"/>
0605	<NameType type="Enumeration"
0606	value="UninterpretedTextString"/>
0607	</AttributeValue>
0608	</Attribute>
0609	</ResponsePayload>
0610	</BatchItem>
0611	</ResponseMessage>
0612	# TIME 12
0613	<RequestMessage>
0614	<RequestHeader>
0615	<ProtocolVersion>
0616	<ProtocolVersionMajor type="Integer" value="1"/>
0617	<ProtocolVersionMinor type="Integer" value="0"/>
0618	</ProtocolVersion>
0619	<BatchCount type="Integer" value="1"/>
0620	</RequestHeader>
0621	<BatchItem>
0622	<Operation type="Enumeration" value="Destroy"/>
0623	<RequestPayload>
0624	<UniqueIdentifier type="TextString"
0625	value="\$UNIQUE_IDENTIFIER_1"/>

0620	</RequestPayload>
0621	</BatchItem>
0622	</RequestMessage>
0623	<ResponseMessage>
0624	<ResponseHeader>
0625	<ProtocolVersion>
0626	<ProtocolVersionMajor type="Integer" value="1"/>
0627	<ProtocolVersionMinor type="Integer" value="0"/>
0628	</ProtocolVersion>
0629	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0630	<BatchCount type="Integer" value="1"/>
0631	</ResponseHeader>
0632	<BatchItem>
0633	<Operation type="Enumeration" value="Destroy"/>
0634	<ResultStatus type="Enumeration" value="Success"/>
0635	<ResponsePayload>
0636	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0637	</ResponsePayload>
0638	</BatchItem>
0639	</ResponseMessage>
# TIME 13	
0640	<RequestMessage>
0641	<RequestHeader>
0642	<ProtocolVersion>
0643	<ProtocolVersionMajor type="Integer" value="1"/>
0644	<ProtocolVersionMinor type="Integer" value="0"/>
0645	</ProtocolVersion>
0646	<BatchCount type="Integer" value="1"/>
0647	</RequestHeader>
0648	<BatchItem>
0649	<Operation type="Enumeration" value="Destroy"/>
0650	<RequestPayload>
0651	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0652	</RequestPayload>
0653	</BatchItem>
0654	</RequestMessage>
0655	<ResponseMessage>
0656	<ResponseHeader>
0657	<ProtocolVersion>
0658	<ProtocolVersionMajor type="Integer" value="1"/>
0659	<ProtocolVersionMinor type="Integer" value="0"/>
0660	</ProtocolVersion>
0661	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0662	<BatchCount type="Integer" value="1"/>
0663	</ResponseHeader>
0664	<BatchItem>
0665	<Operation type="Enumeration" value="Destroy"/>
0666	<ResultStatus type="Enumeration" value="Success"/>
0667	<ResponsePayload>
0668	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0669	</ResponsePayload>
0670	</BatchItem>
0671	</ResponseMessage>

0672	# TIME 14
0673	<RequestMessage>
0674	<RequestHeader>
0675	<ProtocolVersion>
0676	<ProtocolVersionMajor type="Integer" value="1"/>
0677	<ProtocolVersionMinor type="Integer" value="0"/>
0678	</ProtocolVersion>
0679	<BatchCount type="Integer" value="1"/>
0680	</BatchCount>
0681	<Operation type="Enumeration" value="Destroy"/>
0682	</Operation>
0683	<RequestPayload>
0684	<UniqueIdentifier type="TextString"
0685	value="\$UNIQUE_IDENTIFIER_2"/>
0686	</UniqueIdentifier>
0687	</RequestPayload>
0688	</BatchItem>
0689	</RequestMessage>
0690	<ResponseMessage>
0691	<ResponseHeader>
0692	<ProtocolVersion>
0693	<ProtocolVersionMajor type="Integer" value="1"/>
0694	<ProtocolVersionMinor type="Integer" value="0"/>
0695	</ProtocolVersion>
0696	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0697	<BatchCount type="Integer" value="1"/>
0698	</BatchCount>
0699	<Operation type="Enumeration" value="Destroy"/>
0700	</Operation>
0701	<ResultStatus type="Enumeration" value="Success"/>
0702	</ResultStatus>
0703	<ResponsePayload>
0704	<UniqueIdentifier type="TextString"
0705	value="\$UNIQUE_IDENTIFIER_2"/>
0706	</UniqueIdentifier>
0707	</ResponsePayload>
0708	</BatchItem>
0709	</ResponseMessage>
0710	# TIME 15
0711	<RequestMessage>
0712	<RequestHeader>
0713	<ProtocolVersion>
0714	<ProtocolVersionMajor type="Integer" value="1"/>
0715	<ProtocolVersionMinor type="Integer" value="0"/>
0716	</ProtocolVersion>
0717	<BatchCount type="Integer" value="1"/>
0718	</BatchCount>
0719	<Operation type="Enumeration" value="Destroy"/>
0720	</Operation>
0721	<RequestPayload>
0722	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
	</UniqueIdentifier>
	</RequestPayload>
	</BatchItem>
	</RequestMessage>
	<ResponseMessage>
	<ResponseHeader>
	<ProtocolVersion>
	<ProtocolVersionMajor type="Integer" value="1"/>

0723	<ProtocolVersionMinor type="Integer" value="0"/>
0724	</ProtocolVersion>
0725	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0726	<BatchCount type="Integer" value="1"/>
0727	</ResponseHeader>
0728	<BatchItem>
0729	<Operation type="Enumeration" value="Destroy"/>
0730	<ResultStatus type="Enumeration" value="Success"/>
0731	<ResponsePayload>
0732	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0733	</ResponsePayload>
0734	</BatchItem>
0735	</ResponseMessage>

220

221 2.1.25 TC-NP-1-10 - Put

222 In this test case the client issues a Create request, whereby the server creates a new symmetric
223 key and returns the Unique Identifier. To clean up, the client then performs a Destroy operation
224 to destroy the key.

225 The server sends Put messages to the client via a separate channel.

226

	# TIME 0
	# [Client-to-Server]
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>

0026	<Attribute>
0027	<AttributeName type="TextString" value="x-ID"/>
0028	<AttributeValue type="TextString" value="TC-NP-1-10"/>
0029	</Attribute>
0030	</TemplateAttribute>
0031	</RequestPayload>
0032	</BatchItem>
0033	</RequestMessage>
0034	# [Client-to-Server]
0035	<ResponseMessage>
0036	<ResponseHeader>
0037	<ProtocolVersion>
0038	<ProtocolVersionMajor type="Integer" value="1"/>
0039	<ProtocolVersionMinor type="Integer" value="0"/>
0040	</ProtocolVersion>
0041	<TimeStamp type="DateTime" value="2013-06-26T05:13:47+00:00"/>
0042	<BatchCount type="Integer" value="1"/>
0043	</ResponseHeader>
0044	<BatchItem>
0045	<Operation type="Enumeration" value="Create"/>
0046	<ResultStatus type="Enumeration" value="Success"/>
0047	<ResponsePayload>
0048	<ObjectType type="Enumeration" value="SymmetricKey"/>
0049	<UniqueIdentifier type="TextString"
0050	value="\$UNIQUE_IDENTIFIER_0"/>
0051	</ResponsePayload>
0052	</BatchItem>
0053	</ResponseMessage>
0054	# TIME 1
0055	# [Server-to-Client]
0056	<RequestMessage>
0057	<RequestHeader>
0058	<ProtocolVersion>
0059	<ProtocolVersionMajor type="Integer" value="1"/>
0060	<ProtocolVersionMinor type="Integer" value="0"/>
0061	</ProtocolVersion>
0062	<BatchCount type="Integer" value="1"/>
0063	</RequestHeader>
0064	<BatchItem>
0065	<Operation type="Enumeration" value="Put"/>
0066	<RequestPayload>
0067	<UniqueIdentifier type="TextString"
0068	value="\$UNIQUE_IDENTIFIER_0"/>
0069	<PutFunction type="Enumeration" value="New"/>
0070	<SymmetricKey>
0071	<KeyBlock>
0072	<KeyFormatType type="Enumeration" value="Raw"/>
0073	<KeyValue>
0074	<KeyMaterial type="ByteString"
0075	value="7546ef6cd37c49806824984477987dle"/>
0076	</KeyValue>
0077	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0078	<CryptographicLength type="Integer" value="128"/>
0079	</KeyBlock>
0080	</SymmetricKey>
0081	<Attribute>
0082	<AttributeName type="TextString" value="x-ID"/>

0077	<AttributeValue type="TextString" value="TC-NP-1-10"/>
0078	</Attribute>
0079	<Attribute>
0080	<AttributeName type="TextString" value="Unique Identifier"/>
0081	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0082	</Attribute>
0083	<Attribute>
0084	<AttributeName type="TextString" value="Object Type"/>
0085	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0086	</Attribute>
0087	<Attribute>
0088	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0089	<AttributeValue type="Enumeration" value="AES"/>
0090	</Attribute>
0091	<Attribute>
0092	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0093	<AttributeValue type="Integer" value="128"/>
0094	</Attribute>
0095	<Attribute>
0096	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0097	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0098	</Attribute>
0099	<Attribute>
0100	<AttributeName type="TextString" value="Digest"/>
0101	<AttributeValue>
0102	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0103	<DigestValue type="ByteString"
	value="7549ecda2cd1569974c3748f223fbc947ce9cabce581497522e4b75e9d6ed
	e81"/>
0104	</AttributeValue>
0105	</Attribute>
0106	<Attribute>
0107	<AttributeName type="TextString" value="Initial Date"/>
0108	<AttributeValue type="DateTime" value="2013-06-
	26T05:13:48+00:00"/>
0109	</Attribute>
0110	<Attribute>
0111	<AttributeName type="TextString" value="Last Change Date"/>
0112	<AttributeValue type="DateTime" value="2013-06-
	26T05:13:48+00:00"/>
0113	</Attribute>
0114	<Attribute>
0115	<AttributeName type="TextString" value="Lease Time"/>
0116	<AttributeValue type="Interval" value="3600"/>
0117	</Attribute>
0118	<Attribute>
0119	<AttributeName type="TextString" value="State"/>
0120	<AttributeValue type="Enumeration" value="PreActive"/>
0121	</Attribute>
0122	</RequestPayload>
0123	</BatchItem>
0124	</RequestMessage>
	# [Server-to-Client]

0125	<ResponseMessage>
0126	<ResponseHeader>
0127	<ProtocolVersion>
0128	<ProtocolVersionMajor type="Integer" value="1"/>
0129	<ProtocolVersionMinor type="Integer" value="0"/>
0130	</ProtocolVersion>
0131	<TimeStamp type="DateTime" value="2013-06-26T05:13:48+00:00"/>
0132	<BatchCount type="Integer" value="1"/>
0133	</ResponseHeader>
0134	<BatchItem>
0135	<Operation type="Enumeration" value="Put"/>
0136	<ResultStatus type="Enumeration" value="Success"/>
0137	<ResponsePayload>
0138	</BatchItem>
0139	</ResponseMessage>
0140	
	# TIME 2
	# [Client-to-Server]
0141	<RequestMessage>
0142	<RequestHeader>
0143	<ProtocolVersion>
0144	<ProtocolVersionMajor type="Integer" value="1"/>
0145	<ProtocolVersionMinor type="Integer" value="0"/>
0146	</ProtocolVersion>
0147	<BatchCount type="Integer" value="1"/>
0148	</RequestHeader>
0149	<BatchItem>
0150	<Operation type="Enumeration" value="Destroy"/>
0151	<RequestPayload>
0152	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0153	</RequestPayload>
0154	</BatchItem>
0155	</RequestMessage>
	# [Client-to-Server]
0156	<ResponseMessage>
0157	<ResponseHeader>
0158	<ProtocolVersion>
0159	<ProtocolVersionMajor type="Integer" value="1"/>
0160	<ProtocolVersionMinor type="Integer" value="0"/>
0161	</ProtocolVersion>
0162	<TimeStamp type="DateTime" value="2013-06-26T05:13:48+00:00"/>
0163	<BatchCount type="Integer" value="1"/>
0164	</ResponseHeader>
0165	<BatchItem>
0166	<Operation type="Enumeration" value="Destroy"/>
0167	<ResultStatus type="Enumeration" value="Success"/>
0168	<ResponsePayload>
0169	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0170	</ResponsePayload>
0171	</BatchItem>
0172	</ResponseMessage>

228 2.1.26 TC-NP-2-10 - Notify & Put

229 This test case tests the import of key using the Register operation. To validate that the
230 registered key is treated the same as a locally created key, an attribute is added to the key and
231 then modified. Finally, the key is destroyed.

232 The server sends Notify and Put messages to the client via a separate channel.

0001	# TIME 0
0002	# [Client-to-Server]
0003	<RequestMessage>
0004	<RequestHeader>
0005	<ProtocolVersion>
0006	<ProtocolVersionMajor type="Integer" value="1"/>
0007	<ProtocolVersionMinor type="Integer" value="0"/>
0008	</ProtocolVersion>
0009	<BatchCount type="Integer" value="1"/>
0010	</BatchCount>
0011	<BatchItem>
0012	<Operation type="Enumeration" value="Register"/>
0013	<RequestPayload>
0014	<ObjectType type="Enumeration" value="SymmetricKey"/>
0015	<TemplateAttribute>
0016	<Attribute>
0017	<AttributeName type="TextString" value="Cryptographic
0018	Usage Mask"/>
0019	<AttributeValue type="Integer" value="Encrypt"/>
0020	</Attribute>
0021	<Attribute>
0022	<AttributeName type="TextString" value="x-ID"/>
0023	<AttributeValue type="TextString" value="TC-NP-2-10"/>
0024	</Attribute>
0025	</TemplateAttribute>
0026	<SymmetricKey>
0027	<KeyBlock>
0028	<KeyFormatType type="Enumeration" value="Raw"/>
0029	<KeyValue>
0030	<KeyMaterial type="ByteString"
0031	value="1122456789abcdef0123456789abcdef"/>
0032	</KeyValue>
0033	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0034	<CryptographicLength type="Integer" value="128"/>
0035	</CryptographicAlgorithm>
0036	</KeyBlock>
0037	</SymmetricKey>
0038	</RequestPayload>
0039	</BatchItem>
0040	</RequestMessage>
0041	# [Client-to-Server]
0042	<ResponseMessage>
0043	<ResponseHeader>
0044	<ProtocolVersion>
0045	<ProtocolVersionMajor type="Integer" value="1"/>
0046	<ProtocolVersionMinor type="Integer" value="0"/>
0047	</ProtocolVersion>
0048	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0049	<BatchCount type="Integer" value="1"/>

0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
	# [Server-to-Client]
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="0"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Put"/>
0063	<RequestPayload>
0064	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0065	<PutFunction type="Enumeration" value="New"/>
0066	<SymmetricKey>
0067	<KeyBlock>
0068	<KeyFormatType type="Enumeration" value="Raw"/>
0069	<KeyValue>
0070	<KeyMaterial type="ByteString"
	value="1122456789abcdef0123456789abcdef"/>
0071	</KeyValue>
0072	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0073	<CryptographicLength type="Integer" value="128"/>
0074	</KeyBlock>
0075	</SymmetricKey>
0076	<Attribute>
0077	<AttributeName type="TextString" value="x-ID"/>
0078	<AttributeValue type="TextString" value="TC-NP-2-10"/>
0079	</Attribute>
0080	<Attribute>
0081	<AttributeName type="TextString" value="Unique Identifier"/>
0082	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0083	</Attribute>
0084	<Attribute>
0085	<AttributeName type="TextString" value="Object Type"/>
0086	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0087	</Attribute>
0088	<Attribute>
0089	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0090	<AttributeValue type="Enumeration" value="AES"/>
0091	</Attribute>
0092	<Attribute>
0093	<AttributeName type="TextString" value="Cryptographic

0094	Length"/>
0095	<AttributeValue type="Integer" value="128"/>
0096	</Attribute>
0097	<Attribute>
0098	<AttributeName type="TextString" value="Cryptographic Usage
0099	Mask"/>
0100	<AttributeValue type="Integer" value="Encrypt"/>
0101	</Attribute>
0102	<Attribute>
0103	<AttributeName type="TextString" value="Digest"/>
0104	<AttributeValue type="TextString" value="SHA_256"/>
0105	<DigestValue type="ByteString"
0106	value="47c01d3851ce2f254d18928526b6126de30cef9a34a4cfbd4648ec3ed21a9
0107	e86"/>
0108	</Attribute>
0109	</Attribute>
0110	<Attribute>
0111	<AttributeName type="TextString" value="Initial Date"/>
0112	<AttributeValue type="DateTime" value="2013-06-
0113	26T05:54:18+00:00"/>
0114	</Attribute>
0115	</Attribute>
0116	<Attribute>
0117	<AttributeName type="TextString" value="Lease Time"/>
0118	<AttributeValue type="Interval" value="3600"/>
0119	</Attribute>
0120	</Attribute>
0121	<Attribute>
0122	<AttributeName type="TextString" value="State"/>
0123	<AttributeValue type="Enumeration" value="PreActive"/>
0124	</Attribute>
0125	</RequestPayload>
0126	</BatchItem>
0127	</RequestMessage>
0128	# [Server-to-Client]
0129	<ResponseMessage>
0130	<ResponseHeader>
0131	<ProtocolVersion>
0132	<ProtocolVersionMajor type="Integer" value="1"/>
0133	<ProtocolVersionMinor type="Integer" value="0"/>
0134	</ProtocolVersion>
0135	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0136	<BatchCount type="Integer" value="1"/>
0137	</ResponseHeader>
0138	<BatchItem>
0139	<Operation type="Enumeration" value="Put"/>
0140	<ResultStatus type="Enumeration" value="Success"/>
0141	<ResponsePayload>
	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>
	# TIME 2
	# [Client-to-Server]

0142	<RequestMessage>
0143	<RequestHeader>
0144	<ProtocolVersion>
0145	<ProtocolVersionMajor type="Integer" value="1"/>
0146	<ProtocolVersionMinor type="Integer" value="0"/>
0147	</ProtocolVersion>
0148	<BatchCount type="Integer" value="1"/>
0149	</RequestHeader>
0150	<BatchItem>
0151	<Operation type="Enumeration" value="AddAttribute"/>
0152	<RequestPayload>
0153	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0154	<Attribute>
0155	<AttributeName type="TextString" value="x-provider"/>
0156	<AttributeValue type="TextString" value="unknown"/>
0157	</Attribute>
0158	</RequestPayload>
0159	</BatchItem>
0160	</RequestMessage>
	# [Client-to-Server]
0161	<ResponseMessage>
0162	<ResponseHeader>
0163	<ProtocolVersion>
0164	<ProtocolVersionMajor type="Integer" value="1"/>
0165	<ProtocolVersionMinor type="Integer" value="0"/>
0166	</ProtocolVersion>
0167	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0168	<BatchCount type="Integer" value="1"/>
0169	</ResponseHeader>
0170	<BatchItem>
0171	<Operation type="Enumeration" value="AddAttribute"/>
0172	<ResultStatus type="Enumeration" value="Success"/>
0173	<ResponsePayload>
0174	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0175	<Attribute>
0176	<AttributeName type="TextString" value="x-provider"/>
0177	<AttributeValue type="TextString" value="unknown"/>
0178	</Attribute>
0179	</ResponsePayload>
0180	</BatchItem>
0181	</ResponseMessage>
	# TIME 3
	# [Server-to-Client]
0182	<RequestMessage>
0183	<RequestHeader>
0184	<ProtocolVersion>
0185	<ProtocolVersionMajor type="Integer" value="1"/>
0186	<ProtocolVersionMinor type="Integer" value="0"/>
0187	</ProtocolVersion>
0188	<BatchCount type="Integer" value="1"/>
0189	</RequestHeader>
0190	<BatchItem>
0191	<Operation type="Enumeration" value="Notify"/>
0192	<RequestPayload>
0193	<UniqueIdentifier type="TextString"

0194	value="\$UNIQUE_IDENTIFIER_0"/>
0195	<Attribute>
0196	<AttributeName type="TextString" value="x-provider"/>
0197	<AttributeValue type="TextString" value="unknown"/>
0198	</Attribute>
0199	<Attribute>
0199	<AttributeName type="TextString" value="Last Change Date"/>
0200	<AttributeValue type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0201	</Attribute>
0202	</RequestPayload>
0203	</BatchItem>
0204	</RequestMessage>
0205	# [Server-to-Client]
0206	<ResponseMessage>
0207	<ResponseHeader>
0208	<ProtocolVersion>
0208	<ProtocolVersionMajor type="Integer" value="1"/>
0209	<ProtocolVersionMinor type="Integer" value="0"/>
0210	</ProtocolVersion>
0211	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0212	<BatchCount type="Integer" value="1"/>
0213	</ResponseHeader>
0214	<BatchItem>
0215	<Operation type="Enumeration" value="Notify"/>
0216	<ResultStatus type="Enumeration" value="Success"/>
0217	<ResponsePayload>
0218	</ResponsePayload>
0219	</BatchItem>
0220	</ResponseMessage>
0221	# TIME 4
0222	# [Client-to-Server]
0223	<RequestMessage>
0224	<RequestHeader>
0225	<ProtocolVersion>
0226	<ProtocolVersionMajor type="Integer" value="1"/>
0227	<ProtocolVersionMinor type="Integer" value="0"/>
0228	</ProtocolVersion>
0229	<BatchCount type="Integer" value="1"/>
0230	</RequestHeader>
0231	<BatchItem>
0232	<Operation type="Enumeration" value="ModifyAttribute"/>
0233	<RequestPayload>
0234	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0235	<Attribute>
0236	<AttributeName type="TextString" value="x-provider"/>
0237	<AttributeValue type="TextString" value="third party"/>
0238	</Attribute>
0239	</RequestPayload>
0240	</BatchItem>
0241	</RequestMessage>
0242	# [Client-to-Server]
0243	<ResponseMessage>
0244	<ResponseHeader>
0245	<ProtocolVersion>

0243	<ProtocolVersionMajor type="Integer" value="1"/>
0244	<ProtocolVersionMinor type="Integer" value="0"/>
0245	</ProtocolVersion>
0246	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0247	<BatchCount type="Integer" value="1"/>
0248	</ResponseHeader>
0249	<BatchItem>
0250	<Operation type="Enumeration" value="ModifyAttribute"/>
0251	<ResultStatus type="Enumeration" value="Success"/>
0252	<ResponsePayload>
0253	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0254	<Attribute>
0255	<AttributeName type="TextString" value="x-provider"/>
0256	<AttributeValue type="TextString" value="third party"/>
0257	</Attribute>
0258	</ResponsePayload>
0259	</BatchItem>
0260	</ResponseMessage>
	# TIME 5
	# [Server-to-Client]
0261	<RequestMessage>
0262	<RequestHeader>
0263	<ProtocolVersion>
0264	<ProtocolVersionMajor type="Integer" value="1"/>
0265	<ProtocolVersionMinor type="Integer" value="0"/>
0266	</ProtocolVersion>
0267	<BatchCount type="Integer" value="1"/>
0268	</RequestHeader>
0269	<BatchItem>
0270	<Operation type="Enumeration" value="Notify"/>
0271	<RequestPayload>
0272	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0273	<Attribute>
0274	<AttributeName type="TextString" value="x-provider"/>
0275	<AttributeValue type="TextString" value="third party"/>
0276	</Attribute>
0277	<Attribute>
0278	<AttributeName type="TextString" value="Last Change Date"/>
0279	<AttributeValue type="DateTime" value="2013-06-
	26T05:54:18+00:00"/>
0280	</Attribute>
0281	</RequestPayload>
0282	</BatchItem>
0283	</RequestMessage>
	# [Server-to-Client]
0284	<ResponseMessage>
0285	<ResponseHeader>
0286	<ProtocolVersion>
0287	<ProtocolVersionMajor type="Integer" value="1"/>
0288	<ProtocolVersionMinor type="Integer" value="0"/>
0289	</ProtocolVersion>
0290	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0291	<BatchCount type="Integer" value="1"/>
0292	</ResponseHeader>
0293	<BatchItem>

0294	<Operation type="Enumeration" value="Notify"/>
0295	<ResultStatus type="Enumeration" value="Success"/>
0296	<ResponsePayload>
0297	</ResponsePayload>
0298	</BatchItem>
0299	</ResponseMessage>
# TIME 6 # [Client-to-Server]	
0300	<RequestMessage>
0301	<RequestHeader>
0302	<ProtocolVersion>
0303	<ProtocolVersionMajor type="Integer" value="1"/>
0304	<ProtocolVersionMinor type="Integer" value="0"/>
0305	</ProtocolVersion>
0306	<BatchCount type="Integer" value="1"/>
0307	</RequestHeader>
0308	<BatchItem>
0309	<Operation type="Enumeration" value="Destroy"/>
0310	<RequestPayload>
0311	<UniqueIdentifier type="TextString"
0312	value="\$UNIQUE_IDENTIFIER_0"/>
0313	</RequestPayload>
0314	</BatchItem>
0315	</RequestMessage>
0316	<ResponseMessage>
0317	<ResponseHeader>
0318	<ProtocolVersion>
0319	<ProtocolVersionMajor type="Integer" value="1"/>
0320	<ProtocolVersionMinor type="Integer" value="0"/>
0321	</ProtocolVersion>
0322	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0323	<BatchCount type="Integer" value="1"/>
0324	</ResponseHeader>
0325	<BatchItem>
0326	<Operation type="Enumeration" value="Destroy"/>
0327	<ResultStatus type="Enumeration" value="Success"/>
0328	<ResponsePayload>
0329	<UniqueIdentifier type="TextString"
0330	value="\$UNIQUE_IDENTIFIER_0"/>
0331	</ResponsePayload>
0332	</BatchItem>
0333	</ResponseMessage>
# TIME 7 # [Server-to-Client]	
0334	<RequestMessage>
0335	<RequestHeader>
0336	<ProtocolVersion>
0337	<ProtocolVersionMajor type="Integer" value="1"/>
0338	<ProtocolVersionMinor type="Integer" value="0"/>
0339	</ProtocolVersion>
0340	<BatchCount type="Integer" value="1"/>
0341	</RequestHeader>
0342	<BatchItem>
0343	<Operation type="Enumeration" value="Notify"/>
0344	<RequestPayload>

0343	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0344	<Attribute>
0345	<AttributeName type="TextString" value="Last Change Date"/>
0346	<AttributeValue type="DateTime" value="2013-06-
	26T05:54:18+00:00"/>
0347	</Attribute>
0348	<Attribute>
0349	<AttributeName type="TextString" value="State"/>
0350	<AttributeValue type="Enumeration" value="Destroyed"/>
0351	</Attribute>
0352	</RequestPayload>
0353	</BatchItem>
0354	</RequestMessage>
	# [Server-to-Client]
0355	<ResponseMessage>
0356	<ResponseHeader>
0357	<ProtocolVersion>
0358	<ProtocolVersionMajor type="Integer" value="1"/>
0359	<ProtocolVersionMinor type="Integer" value="0"/>
0360	</ProtocolVersion>
0361	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0362	<BatchCount type="Integer" value="1"/>
0363	</ResponseHeader>
0364	<BatchItem>
0365	<Operation type="Enumeration" value="Notify"/>
0366	<ResultStatus type="Enumeration" value="Success"/>
0367	<ResponsePayload>
0368	</ResponsePayload>
0369	</BatchItem>
0370	</ResponseMessage>

233

234 2.1.27 TC-ECC-1-10 - Register an ECC Key Pair

235 EC recommended curve is P-256 (secp256r1)

236 - Private Key format ECPrivateKey - <http://tools.ietf.org/html/rfc5915>

237 - Public Key format SubjectPublicKeyInfo - <http://tools.ietf.org/html/rfc5480>

238 Register a EC private key in the ECPrivateKey key format, then register the corresponding public
239 key, in X.509 (SubjectPublicKeyInfo) format, with the Link attribute pointing to the previously
240 registered private key. Then add the Link attribute to the private key, and perform Locate
241 operations to find the public and private keys using the Link attribute. Get both the private and
242 public keys in default format, then destroy both the private and the public key.

243

244 -----BEGIN EC PRIVATE KEY-----
245 MHcCAQEEIJEqDiCPXdc0sYUYR+RlnEWIsW2fO8GtpRDqLJadr570oAoGCCqGSM49
246 AwEHoUQDQgAes0Q5L7cqomf4bX2DfeHZb0lg/8Bc7vPx+ibYVGpkQvPBOX6Smq2N
247 yrJbKCyooc8AvvfLGKD16kRJOjCm0iOyWw==
248 -----END EC PRIVATE KEY-----
249

250 -----BEGIN PUBLIC KEY-----
251 MFkwEwYHkoZIZj0CAQYIKoZIZj0DAQcDQgAes0Q5L7cqomf4bX2DfeHZbOlG/8Bc
252 7vPx+ibYVGpkQvPBOX6Smq2NyrJbKCyooc8AvvfLGKD16kRJOjCm0iOyWw==
253 -----END PUBLIC KEY-----
254

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="PrivateKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Sign"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-ECC-1-10- prikey1"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<PrivateKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="ECPrivateKey"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString" value="30770201010420912a0e208f5dd734b1851847e4659c4588b16d9f3bc1ada 510ea2c969daf9ef4a00a06082a8648ce3d030107a14403420004b344392fb72aa26 7f86d7d837del96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aad8dcab25 b282ca8alc00bef7cb18a0f5ea44493a30a6d223b25b"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0030	<CryptographicLength type="Integer" value="256"/>
0031	</KeyBlock>
0032	</PrivateKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="0"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>

0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="0"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PublicKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0068	<AttributeValue type="Integer" value="Verify"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>
0073	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0075	</AttributeValue>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-ECC-1-10-
	pubkey1"/>
0080	</Attribute>
0081	</TemplateAttribute>
0082	<PublicKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="X_509"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString"
	value="3059301306072a8648ce3d020106082a8648ce3d03010703420004b344392
	fb72aa267f86d7d837de1d96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aa
	d8dcab25b282ca8alc00bef7cb18a0f5ea44493a30a6d223b25b"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0089	<CryptographicLength type="Integer" value="256"/>
0090	</KeyBlock>
0091	</PublicKey>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>

0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="0"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0109	</ResponsePayload>
0110	</BatchItem>
0111	</ResponseMessage>
# TIME 2	
0112	<RequestMessage>
0113	<RequestHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="0"/>
0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="AddAttribute"/>
0122	<RequestPayload>
0123	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Link"/>
0126	<AttributeValue>
0127	<LinkType type="Enumeration" value="PublicKeyLink"/>
0128	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0129	</AttributeValue>
0130	</Attribute>
0131	</RequestPayload>
0132	</BatchItem>
0133	</RequestMessage>
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="0"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="AddAttribute"/>
0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	<UniqueIdentifier type="TextString"

0148	value="\$UNIQUE_IDENTIFIER_0"/>
0149	<Attribute>
0149	<AttributeName type="TextString" value="Link"/>
0150	<AttributeValue>
0151	<LinkType type="Enumeration" value="PublicKeyLink"/>
0152	<LinkedObjectIdentifier type="TextString"
0153	value="\$UNIQUE_IDENTIFIER_1"/>
0153	</AttributeValue>
0154	</Attribute>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
# TIME 3	
0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="0"/>
0163	</ProtocolVersion>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Locate"/>
0168	<RequestPayload>
0169	<Attribute>
0170	<AttributeName type="TextString" value="Object Type"/>
0171	<AttributeValue type="Enumeration" value="PublicKey"/>
0172	</Attribute>
0173	<Attribute>
0174	<AttributeName type="TextString" value="Link"/>
0175	<AttributeValue>
0176	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0177	<LinkedObjectIdentifier type="TextString"
0178	value="\$UNIQUE_IDENTIFIER_0"/>
0178	</AttributeValue>
0179	</Attribute>
0180	</RequestPayload>
0181	</BatchItem>
0182	</RequestMessage>
0183	<ResponseMessage>
0184	<ResponseHeader>
0185	<ProtocolVersion>
0186	<ProtocolVersionMajor type="Integer" value="1"/>
0187	<ProtocolVersionMinor type="Integer" value="0"/>
0188	</ProtocolVersion>
0189	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0190	<BatchCount type="Integer" value="1"/>
0191	</ResponseHeader>
0192	<BatchItem>
0193	<Operation type="Enumeration" value="Locate"/>
0194	<ResultStatus type="Enumeration" value="Success"/>
0195	<ResponsePayload>
0196	<UniqueIdentifier type="TextString"
0197	value="\$UNIQUE_IDENTIFIER_1"/>
0197	</ResponsePayload>
0198	</BatchItem>
0199	</ResponseMessage>

0200 0201 0202 0203 0204 0205 0206 0207 0208 0209 0210 0211 0212 0213 0214 0215 0216 0217 0218 0219 0220 0221 0222 0223 0224	<pre># TIME 4 <RequestMessage> <RequestHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="0"/> </ProtocolVersion> <BatchCount type="Integer" value="1"/> </RequestHeader> <BatchItem> <Operation type="Enumeration" value="Locate"/> <RequestPayload> <Attribute> <AttributeName type="TextString" value="Object Type"/> <AttributeValue type="Enumeration" value="PrivateKey"/> </Attribute> <Attribute> <AttributeName type="TextString" value="Link"/> <AttributeValue> <LinkType type="Enumeration" value="PublicKeyLink"/> <LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> </AttributeValue> </Attribute> </RequestPayload> </BatchItem> </RequestMessage></pre>
0225 0226 0227 0228 0229 0230 0231 0232 0233 0234 0235 0236 0237 0238 0239 0240 0241	<pre><ResponseMessage> <ResponseHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="0"/> </ProtocolVersion> <TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/> <BatchCount type="Integer" value="1"/> </ResponseHeader> <BatchItem> <Operation type="Enumeration" value="Locate"/> <ResultStatus type="Enumeration" value="Success"/> <ResponsePayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/> </ResponsePayload> </BatchItem> </ResponseMessage></pre>
0242 0243 0244 0245 0246 0247 0248 0249 0250 0251 0252	<pre># TIME 5 <RequestMessage> <RequestHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="0"/> </ProtocolVersion> <BatchCount type="Integer" value="1"/> </RequestHeader> <BatchItem> <Operation type="Enumeration" value="Get"/> <RequestPayload></pre>

0253	<UniqueIdentifier type="TextString"
0254	value="\$UNIQUE_IDENTIFIER_0"/>
0255	</RequestPayload>
0256	</BatchItem>
0257	</RequestMessage>
0257	<ResponseMessage>
0258	<ResponseHeader>
0259	<ProtocolVersion>
0260	<ProtocolVersionMajor type="Integer" value="1"/>
0261	<ProtocolVersionMinor type="Integer" value="0"/>
0262	</ProtocolVersion>
0263	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0264	<BatchCount type="Integer" value="1"/>
0265	</ResponseHeader>
0266	<BatchItem>
0267	<Operation type="Enumeration" value="Get"/>
0268	<ResultStatus type="Enumeration" value="Success"/>
0269	<ResponsePayload>
0270	<ObjectType type="Enumeration" value="PrivateKey"/>
0271	<UniqueIdentifier type="TextString"
0272	value="\$UNIQUE_IDENTIFIER_0"/>
0273	<PrivateKey>
0274	<KeyBlock>
0275	<KeyFormatType type="Enumeration" value="ECPrivateKey"/>
0276	<KeyValue>
0277	<KeyMaterial type="ByteString"
0278	value="30770201010420912a0e208f5dd734b1851847e4659c4588b16d9f3bc1ada
0279	510ea2c969daf9ef4a00a06082a8648ce3d030107a14403420004b344392fb72aa26
0280	7f86d7d837de1d96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aad8dcab25
0281	b282ca8a1cf00bef7cb18a0f5ea44493a30a6d223b25b"/>
0282	</KeyValue>
0283	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0284	<CryptographicLength type="Integer" value="256"/>
0285	</KeyBlock>
0286	</PrivateKey>
0287	</ResponsePayload>
0288	</BatchItem>
0289	</ResponseMessage>
0290	# TIME 6
0291	<RequestMessage>
0292	<RequestHeader>
0293	<ProtocolVersion>
0294	<ProtocolVersionMajor type="Integer" value="1"/>
0295	<ProtocolVersionMinor type="Integer" value="0"/>
0296	</ProtocolVersion>
0297	<BatchCount type="Integer" value="1"/>
0298	</RequestHeader>
0299	<BatchItem>
0300	<Operation type="Enumeration" value="Get"/>
	<RequestPayload>
	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
	</RequestPayload>
	</BatchItem>
	</RequestMessage>
	<ResponseMessage>

0301	<ResponseHeader>
0302	<ProtocolVersion>
0303	<ProtocolVersionMajor type="Integer" value="1"/>
0304	<ProtocolVersionMinor type="Integer" value="0"/>
0305	</ProtocolVersion>
0306	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0307	<BatchCount type="Integer" value="1"/>
0308	</ResponseHeader>
0309	<BatchItem>
0310	<Operation type="Enumeration" value="Get"/>
0311	<ResultStatus type="Enumeration" value="Success"/>
0312	<ResponsePayload>
0313	<ObjectType type="Enumeration" value="PublicKey"/>
0314	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0315	<PublicKey>
0316	<KeyBlock>
0317	<KeyFormatType type="Enumeration" value="X_509"/>
0318	<KeyValue>
0319	<KeyMaterial type="ByteString"
	value="3059301306072a8648ce3d020106082a8648ce3d03010703420004b344392
	fb72aa267f86d7d837deld96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aa
	d8dcab25b282ca8alc00bef7cb18a0f5ea44493a30a6d223b25b"/>
0320	</KeyValue>
0321	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0322	<CryptographicLength type="Integer" value="256"/>
0323	</KeyBlock>
0324	</PublicKey>
0325	</ResponsePayload>
0326	</BatchItem>
0327	</ResponseMessage>
	# TIME 7
0328	<RequestMessage>
0329	<RequestHeader>
0330	<ProtocolVersion>
0331	<ProtocolVersionMajor type="Integer" value="1"/>
0332	<ProtocolVersionMinor type="Integer" value="0"/>
0333	</ProtocolVersion>
0334	<BatchCount type="Integer" value="1"/>
0335	</RequestHeader>
0336	<BatchItem>
0337	<Operation type="Enumeration" value="Destroy"/>
0338	<RequestPayload>
0339	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0340	</RequestPayload>
0341	</BatchItem>
0342	</RequestMessage>
0343	<ResponseMessage>
0344	<ResponseHeader>
0345	<ProtocolVersion>
0346	<ProtocolVersionMajor type="Integer" value="1"/>
0347	<ProtocolVersionMinor type="Integer" value="0"/>
0348	</ProtocolVersion>
0349	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0350	<BatchCount type="Integer" value="1"/>
0351	</ResponseHeader>

0352	<BatchItem>
0353	<Operation type="Enumeration" value="Destroy"/>
0354	<ResultStatus type="Enumeration" value="Success"/>
0355	<ResponsePayload>
0356	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0357	</ResponsePayload>
0358	</BatchItem>
0359	</ResponseMessage>
# TIME 8	
0360	<RequestMessage>
0361	<RequestHeader>
0362	<ProtocolVersion>
0363	<ProtocolVersionMajor type="Integer" value="1"/>
0364	<ProtocolVersionMinor type="Integer" value="0"/>
0365	</ProtocolVersion>
0366	<BatchCount type="Integer" value="1"/>
0367	</RequestHeader>
0368	<BatchItem>
0369	<Operation type="Enumeration" value="Destroy"/>
0370	<RequestPayload>
0371	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0372	</RequestPayload>
0373	</BatchItem>
0374	</RequestMessage>
0375	<ResponseMessage>
0376	<ResponseHeader>
0377	<ProtocolVersion>
0378	<ProtocolVersionMajor type="Integer" value="1"/>
0379	<ProtocolVersionMinor type="Integer" value="0"/>
0380	</ProtocolVersion>
0381	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0382	<BatchCount type="Integer" value="1"/>
0383	</ResponseHeader>
0384	<BatchItem>
0385	<Operation type="Enumeration" value="Destroy"/>
0386	<ResultStatus type="Enumeration" value="Success"/>
0387	<ResponsePayload>
0388	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0389	</ResponsePayload>
0390	</BatchItem>
0391	</ResponseMessage>

255

256 2.1.28 TC-ECC-2-10 - Register an ECC Key Pair in PKCS8 Format

257 EC recommended curve is P-256 (secp256r1)

258 - Public Key format SubjectPublicKeyInfo - <http://tools.ietf.org/html/rfc5480>

259 Register a EC private key in PKCS8 key format (with passphrase 'secret' using pbeWithSHAAnd3-
260 KeyTripleDES-CBC), then register the corresponding public key, in X.509 (SubjectPublicKeyInfo)
261 format, with the Link attribute pointing to the previously registered private key. Then add the

262 Link attribute to the private key, and perform Locate operations to find the public and private
263 keys using the Link attribute. Get both the private and public keys in default format, then
264 destroy both the private and the public key.

265

```
266 -----BEGIN ENCRYPTED PRIVATE KEY-----
267 MIGxMBwGCiqGSib3DQEMAQMwDgQIqCAF0cAFxb4CAggABIGQkUySNQqsjKPKt19y
268 g/n+qhaBssolURUH4PBYVpWVUNzqKQhz0MD8/gfBSz1DOU9s7mC97LVgWaeqJTad
269 sOgPsJL3Z4IUuNTWNOMLZtY3jDz4z4grmyYM2c/aJj9eYVu0Ufp6n1lCsdU6HFpn
270 urzWFAsrK+Yt+zpokG+raOoo08kiZ59Fm30ziZPZF4G74GMM
271 -----END ENCRYPTED PRIVATE KEY-----
272
273 -----BEGIN PUBLIC KEY-----
274 MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEs0Q5L7cqomf4bX2DfeHZbOlG/8Bc
275 7vPx+ibYVGpkQvPBOX6Smq2NyrJbKCyooc8AvvfLGKD16kRJOjCm0iOyWw==
276 -----END PUBLIC KEY-----
277
```

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="PrivateKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Sign"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-ECC-2-10- prikey1"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<PrivateKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="PKCS_8"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString" value="3081b1301c060a2a864886f70d010c0103300e04082f2656a336573139020 20800048190eadf76e9cee21053b01c53e175b0e8c4d627c17dalb2df47d8cfb35a0 d7252a9a6488660d61235be735178d0ca8548871567c22803d8f6f6009f05c26429c 83ab72d0f2e7e7870befc3ec746f52d0eccafe34b72a791e9535b34f584b96dc1240 34e8a82df0b5c3e70018f2d4745d66ae6da9398234ebda2ca4d02992613cb377b965 1282c4f3fd0c5a3c5bc33cc3ae0"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>

0030	<CryptographicLength type="Integer" value="256"/>
0031	</KeyBlock>
0032	</PrivateKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="0"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
0053	# TIME 1 <RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="0"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PublicKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0068	<AttributeValue type="Integer" value="Verify"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>
0073	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0075	</AttributeValue>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-ECC-2-10- pubkey1"/>
0080	</Attribute>
0081	</TemplateAttribute>

0082	<PublicKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="X_509"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString"
	value="3059301306072a8648ce3d020106082a8648ce3d03010703420004b344392
	fb72aa267f86d7d837de1d96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aa
	d8dcab25b282ca8a1cf00bef7cb18a0f5ea44493a30a6d223b25b"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0089	<CryptographicLength type="Integer" value="256"/>
0090	</KeyBlock>
0091	</PublicKey>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="0"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0109	</ResponsePayload>
0110	</BatchItem>
0111	</ResponseMessage>
	# TIME 2
0112	<RequestMessage>
0113	<RequestHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="0"/>
0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="AddAttribute"/>
0122	<RequestPayload>
0123	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Link"/>
0126	<AttributeValue>
0127	<LinkType type="Enumeration" value="PublicKeyLink"/>
0128	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0129	</AttributeValue>
0130	</Attribute>
0131	</RequestPayload>

0132	</BatchItem>
0133	</RequestMessage>
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="0"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="AddAttribute"/>
0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	<UniqueIdentifier type="TextString"
0148	value="\$UNIQUE_IDENTIFIER_0"/>
0149	<Attribute>
0150	<AttributeName type="TextString" value="Link"/>
0151	<AttributeValue>
0152	<LinkType type="Enumeration" value="PublicKeyLink"/>
0153	<LinkedObjectIdentifier type="TextString"
0154	value="\$UNIQUE_IDENTIFIER_1"/>
0155	</AttributeValue>
0156	</Attribute>
0157	</ResponsePayload>
0158	</BatchItem>
0159	</ResponseMessage>
0160	# TIME 3
0161	<RequestMessage>
0162	<RequestHeader>
0163	<ProtocolVersion>
0164	<ProtocolVersionMajor type="Integer" value="1"/>
0165	<ProtocolVersionMinor type="Integer" value="0"/>
0166	</ProtocolVersion>
0167	<BatchCount type="Integer" value="1"/>
0168	</RequestHeader>
0169	<BatchItem>
0170	<Operation type="Enumeration" value="Locate"/>
0171	<RequestPayload>
0172	<Attribute>
0173	<AttributeName type="TextString" value="Object Type"/>
0174	<AttributeValue type="Enumeration" value="PublicKey"/>
0175	</Attribute>
0176	<Attribute>
0177	<AttributeName type="TextString" value="Link"/>
0178	<AttributeValue>
0179	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0180	<LinkedObjectIdentifier type="TextString"
0181	value="\$UNIQUE_IDENTIFIER_0"/>
0182	</AttributeValue>
0183	</Attribute>
0184	</RequestPayload>
0185	</BatchItem>
0186	</RequestMessage>
0187	<ResponseMessage>

0184	<ResponseHeader>
0185	<ProtocolVersion>
0186	<ProtocolVersionMajor type="Integer" value="1"/>
0187	<ProtocolVersionMinor type="Integer" value="0"/>
0188	</ProtocolVersion>
0189	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0190	<BatchCount type="Integer" value="1"/>
0191	</ResponseHeader>
0192	<BatchItem>
0193	<Operation type="Enumeration" value="Locate"/>
0194	<ResultStatus type="Enumeration" value="Success"/>
0195	<ResponsePayload>
0196	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0197	</ResponsePayload>
0198	</BatchItem>
0199	</ResponseMessage>
	# TIME 4
0200	<RequestMessage>
0201	<RequestHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="0"/>
0205	</ProtocolVersion>
0206	<BatchCount type="Integer" value="1"/>
0207	</RequestHeader>
0208	<BatchItem>
0209	<Operation type="Enumeration" value="Locate"/>
0210	<RequestPayload>
0211	<Attribute>
0212	<AttributeName type="TextString" value="Object Type"/>
0213	<AttributeValue type="Enumeration" value="PrivateKey"/>
0214	</Attribute>
0215	<Attribute>
0216	<AttributeName type="TextString" value="Link"/>
0217	<AttributeValue>
0218	<LinkType type="Enumeration" value="PublicKeyLink"/>
0219	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0220	</AttributeValue>
0221	</Attribute>
0222	</RequestPayload>
0223	</BatchItem>
0224	</RequestMessage>
0225	<ResponseMessage>
0226	<ResponseHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="0"/>
0230	</ProtocolVersion>
0231	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0232	<BatchCount type="Integer" value="1"/>
0233	</ResponseHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="Locate"/>
0236	<ResultStatus type="Enumeration" value="Success"/>
0237	<ResponsePayload>

0238	<UniqueIdentifier type="TextString"
0239	value="\$UNIQUE_IDENTIFIER_0"/>
0240	</ResponsePayload>
0241	</BatchItem>
0242	</ResponseMessage>
# TIME 5	
0242	<RequestMessage>
0243	<RequestHeader>
0244	<ProtocolVersion>
0245	<ProtocolVersionMajor type="Integer" value="1"/>
0246	<ProtocolVersionMinor type="Integer" value="0"/>
0247	</ProtocolVersion>
0248	<BatchCount type="Integer" value="1"/>
0249	</RequestHeader>
0250	<BatchItem>
0251	<Operation type="Enumeration" value="Get"/>
0252	<RequestPayload>
0253	<UniqueIdentifier type="TextString"
0254	value="\$UNIQUE_IDENTIFIER_0"/>
0255	</RequestPayload>
0256	</BatchItem>
0257	</RequestMessage>
0258	<ResponseMessage>
0259	<ResponseHeader>
0260	<ProtocolVersion>
0261	<ProtocolVersionMajor type="Integer" value="1"/>
0262	<ProtocolVersionMinor type="Integer" value="0"/>
0263	</ProtocolVersion>
0264	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0265	<BatchCount type="Integer" value="1"/>
0266	</ResponseHeader>
0267	<BatchItem>
0268	<Operation type="Enumeration" value="Get"/>
0269	<ResultStatus type="Enumeration" value="Success"/>
0270	<ResponsePayload>
0271	<ObjectType type="Enumeration" value="PrivateKey"/>
0272	<UniqueIdentifier type="TextString"
0273	value="\$UNIQUE_IDENTIFIER_0"/>
0274	<PrivateKey>
0275	<KeyBlock>
0276	<KeyFormatType type="Enumeration" value="PKCS_8"/>
0277	<KeyValue>
0278	<KeyMaterial type="ByteString"
0279	value="3081b1301c060a2a864886f70d010c0103300e04082f2656a336573139020
0280	20800048190eadf76e9cee21053b01c53e175b0e8c4d627c17dalb2df47d8cfb35a0
0281	d7252a9a6488660d61235be735178d0ca8548871567c22803d8f6f6009f05c26429c
0282	83ab72d0f2e7e7870befc3ec746f52d0eccafe34b72a791e9535b34f584b96dc1240
0283	34e8a82df0b5c3e70018f2d4745d66ae6da9398234ebda2ca4d02992613cb377b965
0284	1282c4f3fd0c5a3c5bc33cc3ae0"/>
0285	</KeyValue>
0286	</KeyBlock>
0287	</PrivateKey>
0288	</ResponsePayload>
0289	</BatchItem>
0290	</ResponseMessage>

0285	# TIME 6
0286	<RequestMessage>
0287	<RequestHeader>
0288	<ProtocolVersion>
0289	<ProtocolVersionMajor type="Integer" value="1"/>
0290	<ProtocolVersionMinor type="Integer" value="0"/>
0291	</ProtocolVersion>
0292	<BatchCount type="Integer" value="1"/>
0293	</BatchCount>
0294	<Operation type="Enumeration" value="Get"/>
0295	<RequestPayload>
0296	<UniqueIdentifier type="TextString"
0297	value="\$UNIQUE_IDENTIFIER_1"/>
0298	</RequestPayload>
0299	</BatchItem>
0300	</RequestMessage>
0301	<ResponseMessage>
0302	<ResponseHeader>
0303	<ProtocolVersion>
0304	<ProtocolVersionMajor type="Integer" value="1"/>
0305	<ProtocolVersionMinor type="Integer" value="0"/>
0306	</ProtocolVersion>
0307	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0308	<BatchCount type="Integer" value="1"/>
0309	</BatchCount>
0310	<Operation type="Enumeration" value="Get"/>
0311	<ResultStatus type="Enumeration" value="Success"/>
0312	<ResponsePayload>
0313	<ObjectType type="Enumeration" value="PublicKey"/>
0314	<UniqueIdentifier type="TextString"
0315	value="\$UNIQUE_IDENTIFIER_1"/>
0316	<PublicKey>
0317	<KeyBlock>
0318	<KeyFormatType type="Enumeration" value="X_509"/>
0319	<KeyValue>
0320	<KeyMaterial type="ByteString"
0321	value="3059301306072a8648ce3d020106082a8648ce3d03010703420004b344392
0322	fb72aa267f86d7d837de1d96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aa
0323	d8dcab25b282ca8alcf00bef7cb18a0f5ea44493a30a6d223b25b"/>
0324	</KeyValue>
0325	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0326	<CryptographicLength type="Integer" value="256"/>
0327	</KeyBlock>
0328	</PublicKey>
0329	</ResponsePayload>
0330	</BatchItem>
0331	</ResponseMessage>
0332	# TIME 7
0333	<RequestMessage>
0334	<RequestHeader>
0335	<ProtocolVersion>
0336	<ProtocolVersionMajor type="Integer" value="1"/>
0337	<ProtocolVersionMinor type="Integer" value="0"/>
0338	</ProtocolVersion>
0339	<BatchCount type="Integer" value="1"/>

0335	</RequestHeader>
0336	<BatchItem>
0337	<Operation type="Enumeration" value="Destroy"/>
0338	<RequestPayload>
0339	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0340	</RequestPayload>
0341	</BatchItem>
0342	</RequestMessage>
0343	<ResponseMessage>
0344	<ResponseHeader>
0345	<ProtocolVersion>
0346	<ProtocolVersionMajor type="Integer" value="1"/>
0347	<ProtocolVersionMinor type="Integer" value="0"/>
0348	</ProtocolVersion>
0349	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0350	<BatchCount type="Integer" value="1"/>
0351	</ResponseHeader>
0352	<BatchItem>
0353	<Operation type="Enumeration" value="Destroy"/>
0354	<ResultStatus type="Enumeration" value="Success"/>
0355	<ResponsePayload>
0356	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0357	</ResponsePayload>
0358	</BatchItem>
0359	</ResponseMessage>
	# TIME 8
0360	<RequestMessage>
0361	<RequestHeader>
0362	<ProtocolVersion>
0363	<ProtocolVersionMajor type="Integer" value="1"/>
0364	<ProtocolVersionMinor type="Integer" value="0"/>
0365	</ProtocolVersion>
0366	<BatchCount type="Integer" value="1"/>
0367	</RequestHeader>
0368	<BatchItem>
0369	<Operation type="Enumeration" value="Destroy"/>
0370	<RequestPayload>
0371	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0372	</RequestPayload>
0373	</BatchItem>
0374	</RequestMessage>
0375	<ResponseMessage>
0376	<ResponseHeader>
0377	<ProtocolVersion>
0378	<ProtocolVersionMajor type="Integer" value="1"/>
0379	<ProtocolVersionMinor type="Integer" value="0"/>
0380	</ProtocolVersion>
0381	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0382	<BatchCount type="Integer" value="1"/>
0383	</ResponseHeader>
0384	<BatchItem>
0385	<Operation type="Enumeration" value="Destroy"/>
0386	<ResultStatus type="Enumeration" value="Success"/>

0387	<ResponsePayload>
0388	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0389	</ResponsePayload>
0390	</BatchItem>
0391	</ResponseMessage>

278

279 2.1.29 TC-ECC-3-10 - Register an ECC Key Pair and ECDSA Certificate

280 EC recommended curve is P-256 (secp256r1)

281 - Private Key format ECPrivateKey - <http://tools.ietf.org/html/rfc5915>

282 - Public Key format SubjectPublicKeyInfo - <http://tools.ietf.org/html/rfc5480>

283 Register a EC private key in the ECPrivateKey key format, then register the corresponding public
284 key, in X.509 (SubjectPublicKeyInfo) format, and a corresponding ECDSA certificate, with the
285 Link attribute pointing to the previously registered private key. Return the attribute values for
286 the ECDSA certificate showing the correct server parsing of the certificate. Then add the Link
287 attribute to the private key, and perform Locate operations to find the public and private keys
288 using the Link attribute. Get both the private and public keys in default format, then destroy
289 both the private and the public key.

290

```
291 -----BEGIN EC PRIVATE KEY-----
292 MHcCAQEEIJEqDiCPXdc0sYUYR+RlnEWIsw2f08GtpRDqLJadr570oAoGCCqGSM49
293 AwEHoUQDQgAes0Q5L7cqomf4bX2DfeHZbOlG/8Bc7vPx+ibYVGpkQvPBOX6Smq2N
294 yrJbKCyooc8AvvfLGKD16kRJOjCm0iOyWw==
295 -----END EC PRIVATE KEY-----
296
297 -----BEGIN PUBLIC KEY-----
298 MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAes0Q5L7cqomf4bX2DfeHZbOlG/8Bc
299 7vPx+ibYVGpkQvPBOX6Smq2NyrJbKCyooc8AvvfLGKD16kRJOjCm0iOyWw==
300 -----END PUBLIC KEY-----
301
302 -----BEGIN CERTIFICATE-----
303 MIIB1zCCAX2gAwIBAgIJANraFqWKNSTZMAoGCCqGSM49BAMCEGxCzAJBgNVBAYT
304 AlVTMQ0wCwYDVQQKQDARURVNUMQ4wDAYDVQQQLDAPQVNJUzEaMBGGA1UEAwRS01J
305 UC1FQy1zZWNNwMjU2cjEwHhcNMjMwNjI0MDM1NDQzWhcNMjMwNjI0MDM1NDQzWjBI
306 MQswCQYDVQQGEwJVUzENMAwGA1UECgwEVEVTVDEOMAwGA1UECwwFT0FTSVMxGjAY
307 BgNVBAMMEUtNSVAtRUMtc2VjZDI1NnIxMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcD
308 QgAes0Q5L7cqomf4bX2DfeHZbOlG/8Bc7vPx+ibYVGpkQvPBOX6Smq2NyrJbKCyo
309 oc8AvvfLGKD16kRJOjCm0iOyW6NQME4wHQYDVR0OBBYEFMDL251FazsUho/ZyIZ9
310 4Pzf79STMB8GA1UdIwQYMBAAFMdL251FazsUho/ZyIZ94Pzf79STMAwGA1UdEwQF
311 MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgI19fyzd1lgavOhIaeHbOnBoV0ldEmg6q
312 YA+OEmaQS98CIQCpuF4UPYklouwi8hDTVavL3MAX/9Cm82CRf1fshp7RQ==
313 -----END CERTIFICATE-----
314
315
```

0001	# TIME 0 <RequestMessage>
------	------------------------------

0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="PrivateKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Sign"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-ECC-3-10-prikey1"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<PrivateKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="ECPrivateKey"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString" value="30770201010420912a0e208f5dd734b1851847e4659c4588b16d9f3bclada510ea2c969daf9ef4a00a06082a8648ce3d030107a14403420004b344392fb72aa267f86d7d837delld96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aad8dcab25b282ca8alc00bef7cb18a0f5ea44493a30a6d223b25b"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0030	<CryptographicLength type="Integer" value="256"/>
0031	</KeyBlock>
0032	</PrivateKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="0"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>

0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="0"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PublicKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0068	<AttributeValue type="Integer" value="Verify"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>
0073	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0075	</AttributeValue>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-ECC-3-10-pubkey1"/>
0080	</Attribute>
0081	</TemplateAttribute>
0082	<PublicKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="X_509"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString" value="3059301306072a8648ce3d020106082a8648ce3d03010703420004b344392fb72aa267f86d7d837de1d96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aad8dcab25b282ca8alc00bef7cb18a0f5ea44493a30a6d223b25b"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0089	<CryptographicLength type="Integer" value="256"/>
0090	</KeyBlock>
0091	</PublicKey>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="0"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>

0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0109	</ResponsePayload>
0110	</BatchItem>
0111	</ResponseMessage>
0112	# TIME 2
0112	<RequestMessage>
0113	<RequestHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="0"/>
0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="Register"/>
0122	<RequestPayload>
0123	<ObjectType type="Enumeration" value="Certificate"/>
0124	<TemplateAttribute>
0125	<Attribute>
0126	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0127	<AttributeValue type="Integer" value="Verify Sign"/>
0128	</Attribute>
0129	<Attribute>
0130	<AttributeName type="TextString" value="Link"/>
0131	<AttributeValue>
0132	<LinkType type="Enumeration" value="PublicKeyLink"/>
0133	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0134	</AttributeValue>
0135	</Attribute>
0136	<Attribute>
0137	<AttributeName type="TextString" value="x-ID"/>
0138	<AttributeValue type="TextString" value="TC-ECC-3-10-
	cert1"/>
0139	</Attribute>
0140	</TemplateAttribute>
0141	<Certificate>
0142	<CertificateType type="Enumeration" value="X_509"/>
0143	<CertificateValue type="ByteString"
	value="308201d73082017da003020102020900dada16a58d2924d9300a06082a864
	8ce3d0403023048310b3009060355040613025553310d300b060355040a0c0454455
	354310e300c060355040b0c054f41534953311a301806035504030c114b4d49502d4
	5432d736563703235367231301e170d3133303632363033353434335a170d3233303
	632343033353434335a3048310b3009060355040613025553310d300b060355040a0
	c0454455354310e300c060355040b0c054f41534953311a301806035504030c114b4
	d49502d45432d7365637032353672313059301306072a8648ce3d020106082a8648c
	e3d03010703420004b344392fb72aa267f86d7d837de1d96ce960ffc05ceef3f1fa2
	6d8546a6442f3c1397e929aad8dcab25b282ca8a1cf00bef7cb18a0f5ea44493a30a
	6d223b25ba350304e301d0603551d0e04160414c74bdb9d456b3b14868fd9c8867de

0144	0fcdfe9d493301f0603551d23041830168014c74bdb9d456b3b14868fd9c8867de0f
0145	cdfe9d493300c0603551d13040530030101ff300a06082a8648ce3d0403020348003
0146	0450220235f5fcb375dd606af3a121a7876ce9c1a15d257449a0eaa600f8e1266904
0147	bdf022100a9b85e143d8925a2ebb08bc8434d56af2f73005fff429bcd8245fd5fb21
0148	a7b45"/>
0149	</Certificate>
0150	</RequestPayload>
0151	</BatchItem>
0152	</RequestMessage>
0153	<ResponseMessage>
0154	<ResponseHeader>
0155	<ProtocolVersion>
0156	<ProtocolVersionMajor type="Integer" value="1"/>
0157	<ProtocolVersionMinor type="Integer" value="0"/>
0158	</ProtocolVersion>
0159	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0160	<BatchCount type="Integer" value="1"/>
0161	</ResponseHeader>
0162	<BatchItem>
0163	<Operation type="Enumeration" value="Register"/>
0164	<ResultStatus type="Enumeration" value="Success"/>
0165	<ResponsePayload>
0166	<UniqueIdentifier type="TextString"
0167	value="\$UNIQUE_IDENTIFIER_2"/>
0168	</ResponsePayload>
0169	</BatchItem>
0170	</ResponseMessage>
0171	# TIME 3
0172	<RequestMessage>
0173	<RequestHeader>
0174	<ProtocolVersion>
0175	<ProtocolVersionMajor type="Integer" value="1"/>
0176	<ProtocolVersionMinor type="Integer" value="0"/>
0177	</ProtocolVersion>
0178	<BatchCount type="Integer" value="2"/>
0179	</RequestHeader>
0180	<BatchItem>
0181	<Operation type="Enumeration" value="AddAttribute"/>
0182	<UniqueBatchItemID type="ByteString" value="01"/>
0183	<RequestPayload>
0184	<UniqueIdentifier type="TextString"
0185	value="\$UNIQUE_IDENTIFIER_0"/>
0186	<Attribute>
0187	<AttributeName type="TextString" value="Link"/>
0188	<AttributeValue>
0189	<LinkType type="Enumeration" value="PublicKeyLink"/>
0190	<LinkedObjectIdentifier type="TextString"
0191	value="\$UNIQUE_IDENTIFIER_1"/>
0192	</AttributeValue>
0193	</Attribute>
0194	</RequestPayload>
0195	</BatchItem>
0196	<BatchItem>
0197	<Operation type="Enumeration" value="AddAttribute"/>
0198	<UniqueBatchItemID type="ByteString" value="02"/>
0199	<RequestPayload>
0200	<UniqueIdentifier type="TextString"

0192	value="\$UNIQUE_IDENTIFIER_0"/>
0193	<Attribute>
0194	<AttributeName type="TextString" value="Link"/>
0195	<AttributeValue>
0196	<LinkType type="Enumeration" value="CertificateLink"/>
0197	<LinkedObjectIdentifier type="TextString"
0198	value="\$UNIQUE_IDENTIFIER_2"/>
0199	</AttributeValue>
0200	</Attribute>
0201	</RequestPayload>
0202	</BatchItem>
0203	</RequestMessage>
0204	<ResponseMessage>
0205	<ResponseHeader>
0206	<ProtocolVersion>
0207	<ProtocolVersionMajor type="Integer" value="1"/>
0208	<ProtocolVersionMinor type="Integer" value="0"/>
0209	</ProtocolVersion>
0210	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0211	<BatchCount type="Integer" value="2"/>
0212	</ResponseHeader>
0213	<BatchItem>
0214	<Operation type="Enumeration" value="AddAttribute"/>
0215	<UniqueBatchItemID type="ByteString" value="01"/>
0216	<ResultStatus type="Enumeration" value="Success"/>
0217	<ResponsePayload>
0218	<UniqueIdentifier type="TextString"
0219	value="\$UNIQUE_IDENTIFIER_0"/>
0220	<Attribute>
0221	<AttributeName type="TextString" value="Link"/>
0222	<AttributeValue>
0223	<LinkType type="Enumeration" value="PublicKeyLink"/>
0224	<LinkedObjectIdentifier type="TextString"
0225	value="\$UNIQUE_IDENTIFIER_1"/>
0226	</AttributeValue>
0227	</Attribute>
0228	</ResponsePayload>
0229	</BatchItem>
0230	<BatchItem>
0231	<Operation type="Enumeration" value="AddAttribute"/>
0232	<UniqueBatchItemID type="ByteString" value="02"/>
0233	<ResultStatus type="Enumeration" value="Success"/>
0234	<ResponsePayload>
0235	<UniqueIdentifier type="TextString"
0236	value="\$UNIQUE_IDENTIFIER_0"/>
0237	<Attribute>
0238	<AttributeName type="TextString" value="Link"/>
0239	<AttributeIndex type="Integer" value="1"/>
0240	<AttributeValue>
0241	<LinkType type="Enumeration" value="CertificateLink"/>
0242	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
	</AttributeValue>
	</Attribute>
	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>

0243 0244 0245 0246 0247 0248 0249 0250 0251 0252 0253 0254 0255 0256 0257	<pre># TIME 4 <RequestMessage> <RequestHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="0"/> </ProtocolVersion> <BatchCount type="Integer" value="1"/> </RequestHeader> <BatchItem> <Operation type="Enumeration" value="GetAttributeList"/> <RequestPayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/> </RequestPayload> </BatchItem> </RequestMessage></pre>
0258 0259 0260 0261 0262 0263 0264 0265 0266 0267 0268 0269 0270 0271 0272 0273 0274 0275 0276 0277 0278 0279 0280 0281 0282 0283 0284 0285 0286 0287 0288	<pre><ResponseMessage> <ResponseHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="0"/> </ProtocolVersion> <TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/> <BatchCount type="Integer" value="1"/> </ResponseHeader> <BatchItem> <Operation type="Enumeration" value="GetAttributeList"/> <ResultStatus type="Enumeration" value="Success"/> <ResponsePayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/> <AttributeName type="TextString" value="x-ID"/> <AttributeName type="TextString" value="Unique Identifier"/> <AttributeName type="TextString" value="Object Type"/> <AttributeName type="TextString" value="Certificate Type"/> <AttributeName type="TextString" value="Certificate Identifier"/> <AttributeName type="TextString" value="Certificate Issuer"/> <AttributeName type="TextString" value="Certificate Subject"/> <AttributeName type="TextString" value="Cryptographic Usage Mask"/> <AttributeName type="TextString" value="Digest"/> <AttributeName type="TextString" value="Initial Date"/> <AttributeName type="TextString" value="Last Change Date"/> <AttributeName type="TextString" value="Lease Time"/> <AttributeName type="TextString" value="Link"/> <AttributeName type="TextString" value="State"/> </ResponsePayload> </BatchItem> </ResponseMessage></pre>
0289 0290 0291 0292 0293	<pre># TIME 5 <RequestMessage> <RequestHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="0"/></pre>

0294	</ProtocolVersion>
0295	<BatchCount type="Integer" value="1"/>
0296	</RequestHeader>
0297	<BatchItem>
0298	<Operation type="Enumeration" value="GetAttributes"/>
0299	<RequestPayload>
0300	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0301	<AttributeName type="TextString" value="Certificate Type"/>
0302	<AttributeName type="TextString" value="Certificate
	Identifier"/>
0303	<AttributeName type="TextString" value="Certificate Issuer"/>
0304	<AttributeName type="TextString" value="Certificate Subject"/>
0305	</RequestPayload>
0306	</BatchItem>
0307	</RequestMessage>
0308	<ResponseMessage>
0309	<ResponseHeader>
0310	<ProtocolVersion>
0311	<ProtocolVersionMajor type="Integer" value="1"/>
0312	<ProtocolVersionMinor type="Integer" value="0"/>
0313	</ProtocolVersion>
0314	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0315	<BatchCount type="Integer" value="1"/>
0316	</ResponseHeader>
0317	<BatchItem>
0318	<Operation type="Enumeration" value="GetAttributes"/>
0319	<ResultStatus type="Enumeration" value="Success"/>
0320	<ResponsePayload>
0321	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0322	<Attribute>
0323	<AttributeName type="TextString" value="Certificate Type"/>
0324	<AttributeValue type="Enumeration" value="X_509"/>
0325	</Attribute>
0326	<Attribute>
0327	<AttributeName type="TextString" value="Certificate
	Identifier"/>
0328	<AttributeValue>
0329	<Issuer type="TextString" value="CN=KMIP-EC-
	secp256r1,OU=OASIS,O=TEST,C=US"/>
0330	<SerialNumber type="TextString" value="DADA16A58D2924D9"/>
0331	</AttributeValue>
0332	</Attribute>
0333	<Attribute>
0334	<AttributeName type="TextString" value="Certificate
	Issuer"/>
0335	<AttributeValue>
0336	<CertificateIssuerDistinguishedName type="TextString"
	value="CN=KMIP-EC-secp256r1,OU=OASIS,O=TEST,C=US"/>
0337	</AttributeValue>
0338	</Attribute>
0339	<Attribute>
0340	<AttributeName type="TextString" value="Certificate
	Subject"/>
0341	<AttributeValue>
0342	<CertificateSubjectDistinguishedName type="TextString"

0343	value="CN=KMIP-EC-secp256r1,OU=OASIS,O=TEST,C=US"/>
0344	</AttributeValue>
0345	</Attribute>
0346	</ResponsePayload>
0347	</BatchItem>
0348	</ResponseMessage>
# TIME 6	
0348	<RequestMessage>
0349	<RequestHeader>
0350	<ProtocolVersion>
0351	<ProtocolVersionMajor type="Integer" value="1"/>
0352	<ProtocolVersionMinor type="Integer" value="0"/>
0353	</ProtocolVersion>
0354	<BatchCount type="Integer" value="1"/>
0355	</RequestHeader>
0356	<BatchItem>
0357	<Operation type="Enumeration" value="Locate"/>
0358	<RequestPayload>
0359	<Attribute>
0360	<AttributeName type="TextString" value="Object Type"/>
0361	<AttributeValue type="Enumeration" value="PublicKey"/>
0362	</Attribute>
0363	<Attribute>
0364	<AttributeName type="TextString" value="Link"/>
0365	<AttributeValue>
0366	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0367	<LinkedObjectIdentifier type="TextString"
0368	value="\$UNIQUE_IDENTIFIER_0"/>
0369	</AttributeValue>
0370	</Attribute>
0371	</RequestPayload>
0372	</BatchItem>
0373	</RequestMessage>
0374	<ResponseMessage>
0375	<ResponseHeader>
0376	<ProtocolVersion>
0377	<ProtocolVersionMajor type="Integer" value="1"/>
0378	<ProtocolVersionMinor type="Integer" value="0"/>
0379	</ProtocolVersion>
0380	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0381	<BatchCount type="Integer" value="1"/>
0382	</ResponseHeader>
0383	<BatchItem>
0384	<Operation type="Enumeration" value="Locate"/>
0385	<ResultStatus type="Enumeration" value="Success"/>
0386	<ResponsePayload>
0387	<UniqueIdentifier type="TextString"
0388	value="\$UNIQUE_IDENTIFIER_1"/>
0389	</ResponsePayload>
0390	</BatchItem>
0391	</ResponseMessage>
# TIME 7	
0390	<RequestMessage>
0391	<RequestHeader>
0392	<ProtocolVersion>
0393	<ProtocolVersionMajor type="Integer" value="1"/>

0394	<ProtocolVersionMinor type="Integer" value="0"/>
0395	</ProtocolVersion>
0396	<BatchCount type="Integer" value="1"/>
0397	</RequestHeader>
0398	<BatchItem>
0399	<Operation type="Enumeration" value="Locate"/>
0400	<RequestPayload>
0401	<Attribute>
0402	<AttributeName type="TextString" value="Object Type"/>
0403	<AttributeValue type="Enumeration" value="PrivateKey"/>
0404	</Attribute>
0405	<Attribute>
0406	<AttributeName type="TextString" value="Link"/>
0407	<AttributeValue>
0408	<LinkType type="Enumeration" value="PublicKeyLink"/>
0409	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0410	</AttributeValue>
0411	</Attribute>
0412	</RequestPayload>
0413	</BatchItem>
0414	</RequestMessage>
0415	<ResponseMessage>
0416	<ResponseHeader>
0417	<ProtocolVersion>
0418	<ProtocolVersionMajor type="Integer" value="1"/>
0419	<ProtocolVersionMinor type="Integer" value="0"/>
0420	</ProtocolVersion>
0421	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0422	<BatchCount type="Integer" value="1"/>
0423	</ResponseHeader>
0424	<BatchItem>
0425	<Operation type="Enumeration" value="Locate"/>
0426	<ResultStatus type="Enumeration" value="Success"/>
0427	<ResponsePayload>
0428	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0429	</ResponsePayload>
0430	</BatchItem>
0431	</ResponseMessage>
	# TIME 8
0432	<RequestMessage>
0433	<RequestHeader>
0434	<ProtocolVersion>
0435	<ProtocolVersionMajor type="Integer" value="1"/>
0436	<ProtocolVersionMinor type="Integer" value="0"/>
0437	</ProtocolVersion>
0438	<BatchCount type="Integer" value="1"/>
0439	</RequestHeader>
0440	<BatchItem>
0441	<Operation type="Enumeration" value="Get"/>
0442	<RequestPayload>
0443	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0444	</RequestPayload>
0445	</BatchItem>
0446	</RequestMessage>

0447	<ResponseMessage>
0448	<ResponseHeader>
0449	<ProtocolVersion>
0450	<ProtocolVersionMajor type="Integer" value="1"/>
0451	<ProtocolVersionMinor type="Integer" value="0"/>
0452	</ProtocolVersion>
0453	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0454	<BatchCount type="Integer" value="1"/>
0455	</ResponseHeader>
0456	<BatchItem>
0457	<Operation type="Enumeration" value="Get"/>
0458	<ResultStatus type="Enumeration" value="Success"/>
0459	<ResponsePayload>
0460	<ObjectType type="Enumeration" value="PrivateKey"/>
0461	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0462	<PrivateKey>
0463	<KeyBlock>
0464	<KeyFormatType type="Enumeration" value="ECPrivateKey"/>
0465	<KeyValue>
0466	<KeyMaterial type="ByteString"
	value="3081b1301c060a2a864886f70d010c0103300e04082f2656a336573139020
	20800048190eadf76e9cee21053b01c53e175b0e8c4d627c17da1b2df47d8cfb35a0
	d7252a9a6488660d61235be735178d0ca8548871567c22803d8f6f6009f05c26429c
	83ab72d0f2e7e7870befc3ec746f52d0eccafe34b72a791e9535b34f584b96dc1240
	34e8a82df0b5c3e70018f2d4745d66ae6da9398234ebda2ca4d02992613cb377b965
	1282c4f3fd0c5a3c5bc33cc3ae0"/>
0467	</KeyValue>
0468	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0469	<CryptographicLength type="Integer" value="256"/>
0470	</KeyBlock>
0471	</PrivateKey>
0472	</ResponsePayload>
0473	</BatchItem>
0474	</ResponseMessage>
	# TIME 9
0475	<RequestMessage>
0476	<RequestHeader>
0477	<ProtocolVersion>
0478	<ProtocolVersionMajor type="Integer" value="1"/>
0479	<ProtocolVersionMinor type="Integer" value="0"/>
0480	</ProtocolVersion>
0481	<BatchCount type="Integer" value="1"/>
0482	</RequestHeader>
0483	<BatchItem>
0484	<Operation type="Enumeration" value="Get"/>
0485	<RequestPayload>
0486	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0487	</RequestPayload>
0488	</BatchItem>
0489	</RequestMessage>
0490	<ResponseMessage>
0491	<ResponseHeader>
0492	<ProtocolVersion>
0493	<ProtocolVersionMajor type="Integer" value="1"/>
0494	<ProtocolVersionMinor type="Integer" value="0"/>

0495	</ProtocolVersion>
0496	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0497	<BatchCount type="Integer" value="1"/>
0498	</ResponseHeader>
0499	<BatchItem>
0500	<Operation type="Enumeration" value="Get"/>
0501	<ResultStatus type="Enumeration" value="Success"/>
0502	<ResponsePayload>
0503	<ObjectType type="Enumeration" value="PublicKey"/>
0504	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0505	<PublicKey>
0506	<KeyBlock>
0507	<KeyFormatType type="Enumeration" value="X_509"/>
0508	<KeyValue>
0509	<KeyMaterial type="ByteString"
	value="3059301306072a8648ce3d020106082a8648ce3d03010703420004b344392fb72aa267f86d7d837de1d96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aad8dcab25b282ca8a1cf00bef7cb18a0f5ea44493a30a6d223b25b"/>
0510	</KeyValue>
0511	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0512	<CryptographicLength type="Integer" value="256"/>
0513	</KeyBlock>
0514	</PublicKey>
0515	</ResponsePayload>
0516	</BatchItem>
0517	</ResponseMessage>
	# TIME 10
0518	<RequestMessage>
0519	<RequestHeader>
0520	<ProtocolVersion>
0521	<ProtocolVersionMajor type="Integer" value="1"/>
0522	<ProtocolVersionMinor type="Integer" value="0"/>
0523	</ProtocolVersion>
0524	<BatchCount type="Integer" value="1"/>
0525	</RequestHeader>
0526	<BatchItem>
0527	<Operation type="Enumeration" value="Destroy"/>
0528	<RequestPayload>
0529	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0530	</RequestPayload>
0531	</BatchItem>
0532	</RequestMessage>
0533	<ResponseMessage>
0534	<ResponseHeader>
0535	<ProtocolVersion>
0536	<ProtocolVersionMajor type="Integer" value="1"/>
0537	<ProtocolVersionMinor type="Integer" value="0"/>
0538	</ProtocolVersion>
0539	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0540	<BatchCount type="Integer" value="1"/>
0541	</ResponseHeader>
0542	<BatchItem>
0543	<Operation type="Enumeration" value="Destroy"/>
0544	<ResultStatus type="Enumeration" value="Success"/>
0545	<ResponsePayload>

0546	<UniqueIdentifier type="TextString"
0547	value="\$UNIQUE_IDENTIFIER_0"/>
0548	</ResponsePayload>
0549	</BatchItem>
	</ResponseMessage>
	# TIME 11
0550	<RequestMessage>
0551	<RequestHeader>
0552	<ProtocolVersion>
0553	<ProtocolVersionMajor type="Integer" value="1"/>
0554	<ProtocolVersionMinor type="Integer" value="0"/>
0555	</ProtocolVersion>
0556	<BatchCount type="Integer" value="1"/>
0557	</RequestHeader>
0558	<BatchItem>
0559	<Operation type="Enumeration" value="Destroy"/>
0560	<RequestPayload>
0561	<UniqueIdentifier type="TextString"
0562	value="\$UNIQUE_IDENTIFIER_1"/>
0563	</RequestPayload>
0564	</BatchItem>
	</RequestMessage>
0565	<ResponseMessage>
0566	<ResponseHeader>
0567	<ProtocolVersion>
0568	<ProtocolVersionMajor type="Integer" value="1"/>
0569	<ProtocolVersionMinor type="Integer" value="0"/>
0570	</ProtocolVersion>
0571	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0572	<BatchCount type="Integer" value="1"/>
0573	</ResponseHeader>
0574	<BatchItem>
0575	<Operation type="Enumeration" value="Destroy"/>
0576	<ResultStatus type="Enumeration" value="Success"/>
0577	<ResponsePayload>
0578	<UniqueIdentifier type="TextString"
0579	value="\$UNIQUE_IDENTIFIER_1"/>
0580	</ResponsePayload>
0581	</BatchItem>
	</ResponseMessage>
	# TIME 12
0582	<RequestMessage>
0583	<RequestHeader>
0584	<ProtocolVersion>
0585	<ProtocolVersionMajor type="Integer" value="1"/>
0586	<ProtocolVersionMinor type="Integer" value="0"/>
0587	</ProtocolVersion>
0588	<BatchCount type="Integer" value="1"/>
0589	</RequestHeader>
0590	<BatchItem>
0591	<Operation type="Enumeration" value="Destroy"/>
0592	<RequestPayload>
0593	<UniqueIdentifier type="TextString"
0594	value="\$UNIQUE_IDENTIFIER_2"/>
0595	</RequestPayload>
	</BatchItem>

0596	</RequestMessage>
0597	<ResponseMessage>
0598	<ResponseHeader>
0599	<ProtocolVersion>
0600	<ProtocolVersionMajor type="Integer" value="1"/>
0601	<ProtocolVersionMinor type="Integer" value="0"/>
0602	</ProtocolVersion>
0603	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0604	<BatchCount type="Integer" value="1"/>
0605	</ResponseHeader>
0606	<BatchItem>
0607	<Operation type="Enumeration" value="Destroy"/>
0608	<ResultStatus type="Enumeration" value="Success"/>
0609	<ResponsePayload>
0610	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0611	</ResponsePayload>
0612	</BatchItem>
0613	</ResponseMessage>

316

317

318

319 2.2 KMIP 1.1 Test Cases

320 2.2.1 TC-311-11 - Create / Destroy

321 In this test case the client issues a Create request, whereby the server creates a new symmetric
322 key and returns the Unique Identifier. To clean up, the client then performs a Destroy operation
323 to destroy the key.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
	Length"/>

0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="x-ID"/>
0028	<AttributeValue type="TextString" value="TC-311-11"/>
0029	</Attribute>
0030	</TemplateAttribute>
0031	</RequestPayload>
0032	</BatchItem>
0033	</RequestMessage>
0034	<ResponseMessage>
0035	<ResponseHeader>
0036	<ProtocolVersion>
0037	<ProtocolVersionMajor type="Integer" value="1"/>
0038	<ProtocolVersionMinor type="Integer" value="1"/>
0039	</ProtocolVersion>
0040	<TimeStamp type="DateTime" value="2012-04-27T08:12:21+00:00"/>
0041	<BatchCount type="Integer" value="1"/>
0042	</ResponseHeader>
0043	<BatchItem>
0044	<Operation type="Enumeration" value="Create"/>
0045	<ResultStatus type="Enumeration" value="Success"/>
0046	<ResponsePayload>
0047	<ObjectType type="Enumeration" value="SymmetricKey"/>
0048	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0049	</ResponsePayload>
0050	</BatchItem>
0051	</ResponseMessage>
	# TIME 1
0052	<RequestMessage>
0053	<RequestHeader>
0054	<ProtocolVersion>
0055	<ProtocolVersionMajor type="Integer" value="1"/>
0056	<ProtocolVersionMinor type="Integer" value="1"/>
0057	</ProtocolVersion>
0058	<BatchCount type="Integer" value="1"/>
0059	</RequestHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="Destroy"/>
0062	<RequestPayload>
0063	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0064	</RequestPayload>
0065	</BatchItem>
0066	</RequestMessage>
0067	<ResponseMessage>
0068	<ResponseHeader>
0069	<ProtocolVersion>
0070	<ProtocolVersionMajor type="Integer" value="1"/>
0071	<ProtocolVersionMinor type="Integer" value="1"/>

```

0072     </ProtocolVersion>
0073     <TimeStamp type="DateTime" value="2012-04-27T08:12:21+00:00"/>
0074     <BatchCount type="Integer" value="1"/>
0075 </ResponseHeader>
0076 <BatchItem>
0077     <Operation type="Enumeration" value="Destroy"/>
0078     <ResultStatus type="Enumeration" value="Success"/>
0079     <ResponsePayload>
0080         <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0081     </ResponsePayload>
0082 </BatchItem>
0083 </ResponseMessage>

```

324

325 2.2.2 TC-312-11 - Register / Create / Get attributes / Destroy

326 Here the client first registers a template object and then creates a symmetric key using the
327 registered template. To verify that the attributes of the key were set correctly from the
328 template, the client then issues a Get Attributes command, after which it destroys first the key
329 and then the template.

```

# TIME 0
0001 <RequestMessage>
0002 <RequestHeader>
0003     <ProtocolVersion>
0004         <ProtocolVersionMajor type="Integer" value="1"/>
0005         <ProtocolVersionMinor type="Integer" value="1"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008 </RequestHeader>
0009 <BatchItem>
0010     <Operation type="Enumeration" value="Register"/>
0011     <RequestPayload>
0012         <ObjectType type="Enumeration" value="Template"/>
0013         <TemplateAttribute>
0014             <Attribute>
0015                 <AttributeName type="TextString" value="x-ID"/>
0016                 <AttributeValue type="TextString" value="TC-312-11"/>
0017             </Attribute>
0018             <Attribute>
0019                 <AttributeName type="TextString" value="Name"/>
0020                 <AttributeValue>
0021                     <NameValue type="TextString" value="TC-312-11-
template1"/>
0022                     <NameType type="Enumeration"
value="UninterpretedTextString"/>
0023                 </AttributeValue>
0024             </Attribute>
0025         </TemplateAttribute>
0026         <Template>
0027             <Attribute>
0028                 <AttributeName type="TextString" value="Object Group"/>
0029                 <AttributeValue type="TextString" value="Group1"/>
0030             </Attribute>

```

0031	<Attribute>
0032	<AttributeName type="TextString" value="Application Specific Information"/>
0033	<AttributeValue>
0034	<ApplicationNamespace type="TextString" value="ssl"/>
0035	<ApplicationData type="TextString" value="www.example.com"/>
0036	</AttributeValue>
0037	</Attribute>
0038	<Attribute>
0039	<AttributeName type="TextString" value="Contact Information"/>
0040	<AttributeValue type="TextString" value="Joe"/>
0041	</Attribute>
0042	<Attribute>
0043	<AttributeName type="TextString" value="x-Purpose"/>
0044	<AttributeValue type="TextString" value="demonstration"/>
0045	</Attribute>
0046	</Template>
0047	</RequestPayload>
0048	</BatchItem>
0049	</RequestMessage>
0050	<ResponseMessage>
0051	<ResponseHeader>
0052	<ProtocolVersion>
0053	<ProtocolVersionMajor type="Integer" value="1"/>
0054	<ProtocolVersionMinor type="Integer" value="1"/>
0055	</ProtocolVersion>
0056	<TimeStamp type="DateTime" value="2012-04-27T08:12:21+00:00"/>
0057	<BatchCount type="Integer" value="1"/>
0058	</ResponseHeader>
0059	<BatchItem>
0060	<Operation type="Enumeration" value="Register"/>
0061	<ResultStatus type="Enumeration" value="Success"/>
0062	<ResponsePayload>
0063	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0064	</ResponsePayload>
0065	</BatchItem>
0066	</ResponseMessage>
	# TIME 1
0067	<RequestMessage>
0068	<RequestHeader>
0069	<ProtocolVersion>
0070	<ProtocolVersionMajor type="Integer" value="1"/>
0071	<ProtocolVersionMinor type="Integer" value="1"/>
0072	</ProtocolVersion>
0073	<BatchCount type="Integer" value="1"/>
0074	</RequestHeader>
0075	<BatchItem>
0076	<Operation type="Enumeration" value="Create"/>
0077	<RequestPayload>
0078	<ObjectType type="Enumeration" value="SymmetricKey"/>
0079	<TemplateAttribute>
0080	<Name>
0081	<NameValue type="TextString" value="TC-312-11-templatel"/>
0082	<NameType type="Enumeration"

0083	value="UninterpretedTextString"/>
0084	</Name>
0085	<Attribute>
0086	<AttributeName type="TextString" value="Cryptographic
0087	Algorithm"/>
0088	<AttributeValue type="Enumeration" value="AES"/>
0089	</Attribute>
0090	<Attribute>
0091	<AttributeName type="TextString" value="Cryptographic
0092	Length"/>
0093	<AttributeValue type="Integer" value="128"/>
0094	</Attribute>
0095	<Attribute>
0096	<AttributeName type="TextString" value="Cryptographic
0097	Usage Mask"/>
0098	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0099	</Attribute>
0100	<Attribute>
0101	<AttributeName type="TextString" value="Name"/>
0102	<AttributeValue>
0103	<NameValue type="TextString" value="TC-312-11-key1"/>
0104	<NameType type="Enumeration"
0105	value="UninterpretedTextString"/>
0106	</AttributeValue>
0107	</Attribute>
0108	</TemplateAttribute>
0109	</RequestPayload>
0110	</BatchItem>
0111	</RequestMessage>
0112	<ResponseMessage>
0113	<ResponseHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="1"/>
0117	</ProtocolVersion>
0118	<TimeStamp type="DateTime" value="2012-04-27T08:12:22+00:00"/>
0119	<BatchCount type="Integer" value="1"/>
0120	</ResponseHeader>
0121	<BatchItem>
0122	<Operation type="Enumeration" value="Create"/>
0123	<ResultStatus type="Enumeration" value="Success"/>
0124	<ResponsePayload>
0125	<ObjectType type="Enumeration" value="SymmetricKey"/>
0126	<UniqueIdentifier type="TextString"
0127	value="\$UNIQUE_IDENTIFIER_1"/>
0128	</ResponsePayload>
0129	</BatchItem>
0130	</ResponseMessage>
0131	# TIME 2
0132	<RequestMessage>
0133	<RequestHeader>
0134	<ProtocolVersion>
0135	<ProtocolVersionMajor type="Integer" value="1"/>
0136	<ProtocolVersionMinor type="Integer" value="1"/>
0137	</ProtocolVersion>
0138	<BatchCount type="Integer" value="1"/>
0139	</RequestHeader>

0133	<BatchItem>
0134	<Operation type="Enumeration" value="GetAttributes"/>
0135	<RequestPayload>
0136	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0137	<AttributeName type="TextString" value="Object Group"/>
0138	<AttributeName type="TextString" value="Application Specific
	Information"/>
0139	<AttributeName type="TextString" value="Contact Information"/>
0140	<AttributeName type="TextString" value="x-Purpose"/>
0141	</RequestPayload>
0142	</BatchItem>
0143	</RequestMessage>
0144	<ResponseMessage>
0145	<ResponseHeader>
0146	<ProtocolVersion>
0147	<ProtocolVersionMajor type="Integer" value="1"/>
0148	<ProtocolVersionMinor type="Integer" value="1"/>
0149	</ProtocolVersion>
0150	<TimeStamp type="DateTime" value="2012-04-27T08:12:22+00:00"/>
0151	<BatchCount type="Integer" value="1"/>
0152	</ResponseHeader>
0153	<BatchItem>
0154	<Operation type="Enumeration" value="GetAttributes"/>
0155	<ResultStatus type="Enumeration" value="Success"/>
0156	<ResponsePayload>
0157	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0158	<Attribute>
0159	<AttributeName type="TextString" value="Object Group"/>
0160	<AttributeValue type="TextString" value="Group1"/>
0161	</Attribute>
0162	<Attribute>
0163	<AttributeName type="TextString" value="Application Specific
	Information"/>
0164	<AttributeValue>
0165	<ApplicationNamespace type="TextString" value="ssl"/>
0166	<ApplicationData type="TextString"
	value="www.example.com"/>
0167	</AttributeValue>
0168	</Attribute>
0169	<Attribute>
0170	<AttributeName type="TextString" value="Contact
	Information"/>
0171	<AttributeValue type="TextString" value="Joe"/>
0172	</Attribute>
0173	<Attribute>
0174	<AttributeName type="TextString" value="x-Purpose"/>
0175	<AttributeValue type="TextString" value="demonstration"/>
0176	</Attribute>
0177	</ResponsePayload>
0178	</BatchItem>
0179	</ResponseMessage>
	# TIME 3
0180	<RequestMessage>
0181	<RequestHeader>
0182	<ProtocolVersion>

0183	<ProtocolVersionMajor type="Integer" value="1"/>
0184	<ProtocolVersionMinor type="Integer" value="1"/>
0185	</ProtocolVersion>
0186	<BatchCount type="Integer" value="1"/>
0187	</RequestHeader>
0188	<BatchItem>
0189	<Operation type="Enumeration" value="Destroy"/>
0190	<RequestPayload>
0191	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0192	</RequestPayload>
0193	</BatchItem>
0194	</RequestMessage>
0195	<ResponseMessage>
0196	<ResponseHeader>
0197	<ProtocolVersion>
0198	<ProtocolVersionMajor type="Integer" value="1"/>
0199	<ProtocolVersionMinor type="Integer" value="1"/>
0200	</ProtocolVersion>
0201	<TimeStamp type="DateTime" value="2012-04-27T08:12:22+00:00"/>
0202	<BatchCount type="Integer" value="1"/>
0203	</ResponseHeader>
0204	<BatchItem>
0205	<Operation type="Enumeration" value="Destroy"/>
0206	<ResultStatus type="Enumeration" value="Success"/>
0207	<ResponsePayload>
0208	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0209	</ResponsePayload>
0210	</BatchItem>
0211	</ResponseMessage>
	# TIME 4
0212	<RequestMessage>
0213	<RequestHeader>
0214	<ProtocolVersion>
0215	<ProtocolVersionMajor type="Integer" value="1"/>
0216	<ProtocolVersionMinor type="Integer" value="1"/>
0217	</ProtocolVersion>
0218	<BatchCount type="Integer" value="1"/>
0219	</RequestHeader>
0220	<BatchItem>
0221	<Operation type="Enumeration" value="Destroy"/>
0222	<RequestPayload>
0223	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0224	</RequestPayload>
0225	</BatchItem>
0226	</RequestMessage>
0227	<ResponseMessage>
0228	<ResponseHeader>
0229	<ProtocolVersion>
0230	<ProtocolVersionMajor type="Integer" value="1"/>
0231	<ProtocolVersionMinor type="Integer" value="1"/>
0232	</ProtocolVersion>
0233	<TimeStamp type="DateTime" value="2012-04-27T08:12:22+00:00"/>
0234	<BatchCount type="Integer" value="1"/>

```

0235 </ResponseHeader>
0236 <BatchItem>
0237   <Operation type="Enumeration" value="Destroy"/>
0238   <ResultStatus type="Enumeration" value="Success"/>
0239   <ResponsePayload>
0240     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0241   </ResponsePayload>
0242 </BatchItem>
0243 </ResponseMessage>

```

330

331 2.2.3 TC-313-11 - Create / Locate / Get / Destroy

332 This test case tests the Locate and Get operations, in addition to the previously used operations
333 Create and Destroy. A symmetric key is first created, and then a lookup is performed on the
334 Name attribute using the Locate operation. Subsequently, a Get request is issued to retrieve the
335 located key, after which the key on the server is destroyed.

```

# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="1"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="Create"/>
0011     <RequestPayload>
0012       <ObjectType type="Enumeration" value="SymmetricKey"/>
0013       <TemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Name"/>
0016           <AttributeValue>
0017             <NameValue type="TextString" value="TC-313-11-key1"/>
0018             <NameType type="Enumeration"
value="UninterpretedTextString"/>
0019           </AttributeValue>
0020         </Attribute>
0021         <Attribute>
0022           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0023           <AttributeValue type="Enumeration" value="DES3"/>
0024         </Attribute>
0025         <Attribute>
0026           <AttributeName type="TextString" value="Cryptographic
Length"/>
0027           <AttributeValue type="Integer" value="168"/>
0028         </Attribute>
0029         <Attribute>
0030           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0031           <AttributeValue type="Integer" value="Decrypt Encrypt"/>

```

0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="1"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2012-04-27T08:12:22+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
0055	# TIME 1
0056	<RequestMessage>
0057	<RequestHeader>
0058	<ProtocolVersion>
0059	<ProtocolVersionMajor type="Integer" value="1"/>
0060	<ProtocolVersionMinor type="Integer" value="1"/>
0061	</ProtocolVersion>
0062	<BatchCount type="Integer" value="1"/>
0063	</RequestHeader>
0064	<BatchItem>
0065	<Operation type="Enumeration" value="Locate"/>
0066	<RequestPayload>
0067	<Attribute>
0068	<AttributeName type="TextString" value="Object Type"/>
0069	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0070	</Attribute>
0071	<Attribute>
0072	<AttributeName type="TextString" value="Name"/>
0073	<AttributeValue>
0074	<NameValue type="TextString" value="TC-313-11-key1"/>
0075	<NameType type="Enumeration"
0076	value="UninterpretedTextString"/>
0077	</AttributeValue>
0078	</Attribute>
0079	</RequestPayload>
0080	</BatchItem>
0081	</RequestMessage>
0082	<ResponseMessage>
0083	<ResponseHeader>
0084	<ProtocolVersion>
	<ProtocolVersionMajor type="Integer" value="1"/>
	<ProtocolVersionMinor type="Integer" value="1"/>

0085	</ProtocolVersion>
0086	<TimeStamp type="DateTime" value="2012-04-27T08:12:22+00:00"/>
0087	<BatchCount type="Integer" value="1"/>
0088	</ResponseHeader>
0089	<BatchItem>
0090	<Operation type="Enumeration" value="Locate"/>
0091	<ResultStatus type="Enumeration" value="Success"/>
0092	<ResponsePayload>
0093	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0094	</ResponsePayload>
0095	</BatchItem>
0096	</ResponseMessage>
# TIME 2	
0097	<RequestMessage>
0098	<RequestHeader>
0099	<ProtocolVersion>
0100	<ProtocolVersionMajor type="Integer" value="1"/>
0101	<ProtocolVersionMinor type="Integer" value="1"/>
0102	</ProtocolVersion>
0103	<BatchCount type="Integer" value="1"/>
0104	</RequestHeader>
0105	<BatchItem>
0106	<Operation type="Enumeration" value="Get"/>
0107	<RequestPayload>
0108	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0109	</RequestPayload>
0110	</BatchItem>
0111	</RequestMessage>
0112	<ResponseMessage>
0113	<ResponseHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="1"/>
0117	</ProtocolVersion>
0118	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0119	<BatchCount type="Integer" value="1"/>
0120	</ResponseHeader>
0121	<BatchItem>
0122	<Operation type="Enumeration" value="Get"/>
0123	<ResultStatus type="Enumeration" value="Success"/>
0124	<ResponsePayload>
0125	<ObjectType type="Enumeration" value="SymmetricKey"/>
0126	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0127	<SymmetricKey>
0128	<KeyBlock>
0129	<KeyFormatType type="Enumeration" value="Raw"/>
0130	<KeyValue>
0131	<KeyMaterial type="ByteString"
	value="7367578051012a6d134a855e25c8cd5e4ca131455729d3c8"/>
0132	</KeyValue>
0133	<CryptographicAlgorithm type="Enumeration" value="DES3"/>
0134	<CryptographicLength type="Integer" value="168"/>
0135	</KeyBlock>
0136	</SymmetricKey>

0137	</ResponsePayload>
0138	</BatchItem>
0139	</ResponseMessage>
# TIME 3	
0140	<RequestMessage>
0141	<RequestHeader>
0142	<ProtocolVersion>
0143	<ProtocolVersionMajor type="Integer" value="1"/>
0144	<ProtocolVersionMinor type="Integer" value="1"/>
0145	</ProtocolVersion>
0146	<BatchCount type="Integer" value="1"/>
0147	</RequestHeader>
0148	<BatchItem>
0149	<Operation type="Enumeration" value="Destroy"/>
0150	<RequestPayload>
0151	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0152	</RequestPayload>
0153	</BatchItem>
0154	</RequestMessage>
0155	<ResponseMessage>
0156	<ResponseHeader>
0157	<ProtocolVersion>
0158	<ProtocolVersionMajor type="Integer" value="1"/>
0159	<ProtocolVersionMinor type="Integer" value="1"/>
0160	</ProtocolVersion>
0161	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0162	<BatchCount type="Integer" value="1"/>
0163	</ResponseHeader>
0164	<BatchItem>
0165	<Operation type="Enumeration" value="Destroy"/>
0166	<ResultStatus type="Enumeration" value="Success"/>
0167	<ResponsePayload>
0168	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0169	</ResponsePayload>
0170	</BatchItem>
0171	</ResponseMessage>
# TIME 4	
0172	<RequestMessage>
0173	<RequestHeader>
0174	<ProtocolVersion>
0175	<ProtocolVersionMajor type="Integer" value="1"/>
0176	<ProtocolVersionMinor type="Integer" value="1"/>
0177	</ProtocolVersion>
0178	<BatchCount type="Integer" value="1"/>
0179	</RequestHeader>
0180	<BatchItem>
0181	<Operation type="Enumeration" value="Locate"/>
0182	<RequestPayload>
0183	<Attribute>
0184	<AttributeName type="TextString" value="Unique Identifier"/>
0185	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0186	</Attribute>
0187	</RequestPayload>

0188	</BatchItem>
0189	</RequestMessage>
0190	<ResponseMessage>
0191	<ResponseHeader>
0192	<ProtocolVersion>
0193	<ProtocolVersionMajor type="Integer" value="1"/>
0194	<ProtocolVersionMinor type="Integer" value="1"/>
0195	</ProtocolVersion>
0196	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0197	<BatchCount type="Integer" value="1"/>
0198	</ResponseHeader>
0199	<BatchItem>
0200	<Operation type="Enumeration" value="Locate"/>
0201	<ResultStatus type="Enumeration" value="Success"/>
0202	<ResponsePayload>
0203	</ResponsePayload>
0204	</BatchItem>
0205	</ResponseMessage>

336

337 2.2.4 TC-314-11 - Dual Client Test Case, ID Placeholder-linked Locate & Get 338 Batch

339 This test case has two clients performing operations on the same key. The first client initially
340 registers a template and creates a symmetric key using that template. The second client then
341 does a batched Locate and Get using the ID Placeholder to retrieve the key. The second client
342 thereafter performs a number of operations on the key (Get Attribute List, Get Attribute, Add
343 Attribute, Modify Attribute and Delete Attribute), before the first client finally destroys the key
344 and the template. The first client also tries to Get the key and the template after they have been
345 destroyed, but the Get operation fails in both cases. This test case demonstrates the fact that it
346 is possible for two clients to cooperate and use the same managed object while only having
347 knowledge of a single pre-agreed Name attribute value and without having to share any other
348 information.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="Template"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Name"/>
0016	<AttributeValue>
0017	<NameValue type="TextString" value="TC-314-11- templatel"/>

0018	<NameType type="Enumeration"
0019	value="UninterpretedTextString"/>
0020	</AttributeValue>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<Template>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Cryptographic
0026	Algorithm"/>
0027	<AttributeValue type="Enumeration" value="AES"/>
0028	</Attribute>
0029	<Attribute type="TextString" value="Cryptographic
0030	Length"/>
0031	<AttributeValue type="Integer" value="128"/>
0032	</Attribute>
0033	</Template>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="1"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Register"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<UniqueIdentifier type="TextString"
0051	value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
0055	# TIME 1
0056	<RequestMessage>
0057	<RequestHeader>
0058	<ProtocolVersion>
0059	<ProtocolVersionMajor type="Integer" value="1"/>
0060	<ProtocolVersionMinor type="Integer" value="1"/>
0061	</ProtocolVersion>
0062	<BatchCount type="Integer" value="1"/>
0063	</RequestHeader>
0064	<BatchItem>
0065	<Operation type="Enumeration" value="Create"/>
0066	<RequestPayload>
0067	<ObjectType type="Enumeration" value="SymmetricKey"/>
0068	<TemplateAttribute>
	<Name>
	<NameValue type="TextString" value="TC-314-11-templatel"/>
	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
	</Name>

0069	<Attribute>
0070	<AttributeName type="TextString" value="Name"/>
0071	<AttributeValue>
0072	<NameValue type="TextString" value="TC-314-11-key1"/>
0073	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0074	</AttributeValue>
0075	</Attribute>
0076	<Attribute>
0077	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0078	<AttributeValue type="Integer" value="Encrypt"/>
0079	</Attribute>
0080	<Attribute>
0081	<AttributeName type="TextString" value="Contact
	Information"/>
0082	<AttributeValue type="TextString" value="Foo"/>
0083	</Attribute>
0084	</TemplateAttribute>
0085	</RequestPayload>
0086	</BatchItem>
0087	</RequestMessage>
0088	<ResponseMessage>
0089	<ResponseHeader>
0090	<ProtocolVersion>
0091	<ProtocolVersionMajor type="Integer" value="1"/>
0092	<ProtocolVersionMinor type="Integer" value="1"/>
0093	</ProtocolVersion>
0094	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0095	<BatchCount type="Integer" value="1"/>
0096	</ResponseHeader>
0097	<BatchItem>
0098	<Operation type="Enumeration" value="Create"/>
0099	<ResultStatus type="Enumeration" value="Success"/>
0100	<ResponsePayload>
0101	<ObjectType type="Enumeration" value="SymmetricKey"/>
0102	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0103	</ResponsePayload>
0104	</BatchItem>
0105	</ResponseMessage>
	# TIME 2
0106	<RequestMessage>
0107	<RequestHeader>
0108	<ProtocolVersion>
0109	<ProtocolVersionMajor type="Integer" value="1"/>
0110	<ProtocolVersionMinor type="Integer" value="1"/>
0111	</ProtocolVersion>
0112	<BatchOrderOption type="Boolean" value="true"/>
0113	<BatchCount type="Integer" value="2"/>
0114	</RequestHeader>
0115	<BatchItem>
0116	<Operation type="Enumeration" value="Locate"/>
0117	<UniqueBatchItemID type="ByteString" value="aa21f8c659d6e10d"/>
0118	<RequestPayload>
0119	<Attribute>
0120	<AttributeName type="TextString" value="Object Type"/>

0121	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0122	</Attribute>
0123	<Attribute>
0124	<AttributeName type="TextString" value="Name"/>
0125	<AttributeValue>
0126	<NameValue type="TextString" value="TC-314-11-key1"/>
0127	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0128	</AttributeValue>
0129	</Attribute>
0130	</RequestPayload>
0131	</BatchItem>
0132	<BatchItem>
0133	<Operation type="Enumeration" value="Get"/>
0134	<UniqueBatchItemID type="ByteString" value="495a95f165854dle"/>
0135	<RequestPayload>
0136	</RequestPayload>
0137	</BatchItem>
0138	</RequestMessage>
0139	<ResponseMessage>
0140	<ResponseHeader>
0141	<ProtocolVersion>
0142	<ProtocolVersionMajor type="Integer" value="1"/>
0143	<ProtocolVersionMinor type="Integer" value="1"/>
0144	</ProtocolVersion>
0145	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0146	<BatchCount type="Integer" value="2"/>
0147	</ResponseHeader>
0148	<BatchItem>
0149	<Operation type="Enumeration" value="Locate"/>
0150	<UniqueBatchItemID type="ByteString" value="aa21f8c659d6e10d"/>
0151	<ResultStatus type="Enumeration" value="Success"/>
0152	<ResponsePayload>
0153	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0154	</ResponsePayload>
0155	</BatchItem>
0156	<BatchItem>
0157	<Operation type="Enumeration" value="Get"/>
0158	<UniqueBatchItemID type="ByteString" value="495a95f165854dle"/>
0159	<ResultStatus type="Enumeration" value="Success"/>
0160	<ResponsePayload>
0161	<ObjectType type="Enumeration" value="SymmetricKey"/>
0162	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0163	<SymmetricKey>
0164	<KeyBlock>
0165	<KeyFormatType type="Enumeration" value="Raw"/>
0166	<KeyValue>
0167	<KeyMaterial type="ByteString"
	value="d351910fld7934d6e2ae17576564e2bc"/>
0168	</KeyValue>
0169	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0170	<CryptographicLength type="Integer" value="128"/>
0171	</KeyBlock>
0172	</SymmetricKey>
0173	</ResponsePayload>

0174	</BatchItem>
0175	</ResponseMessage>
# TIME 3	
0176	<RequestMessage>
0177	<RequestHeader>
0178	<ProtocolVersion>
0179	<ProtocolVersionMajor type="Integer" value="1"/>
0180	<ProtocolVersionMinor type="Integer" value="1"/>
0181	</ProtocolVersion>
0182	<BatchCount type="Integer" value="1"/>
0183	</RequestHeader>
0184	<BatchItem>
0185	<Operation type="Enumeration" value="GetAttributeList"/>
0186	<RequestPayload>
0187	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0188	</RequestPayload>
0189	</BatchItem>
0190	</RequestMessage>
0191	<ResponseMessage>
0192	<ResponseHeader>
0193	<ProtocolVersion>
0194	<ProtocolVersionMajor type="Integer" value="1"/>
0195	<ProtocolVersionMinor type="Integer" value="1"/>
0196	</ProtocolVersion>
0197	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0198	<BatchCount type="Integer" value="1"/>
0199	</ResponseHeader>
0200	<BatchItem>
0201	<Operation type="Enumeration" value="GetAttributeList"/>
0202	<ResultStatus type="Enumeration" value="Success"/>
0203	<ResponsePayload>
0204	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0205	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0206	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0207	<AttributeName type="TextString" value="State"/>
0208	<AttributeName type="TextString" value="Digest"/>
0209	<AttributeName type="TextString" value="Lease Time"/>
0210	<AttributeName type="TextString" value="Initial Date"/>
0211	<AttributeName type="TextString" value="Unique Identifier"/>
0212	<AttributeName type="TextString" value="Name"/>
0213	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0214	<AttributeName type="TextString" value="Object Type"/>
0215	<AttributeName type="TextString" value="Contact Information"/>
0216	<AttributeName type="TextString" value="Last Change Date"/>
0217	<AttributeName type="TextString" value="Fresh"/>
0218	</ResponsePayload>
0219	</BatchItem>
0220	</ResponseMessage>
# TIME 4	
0221	<RequestMessage>
0222	<RequestHeader>

0223	<ProtocolVersion>
0224	<ProtocolVersionMajor type="Integer" value="1"/>
0225	<ProtocolVersionMinor type="Integer" value="1"/>
0226	</ProtocolVersion>
0227	<BatchCount type="Integer" value="1"/>
0228	</RequestHeader>
0229	<BatchItem>
0230	<Operation type="Enumeration" value="GetAttributes"/>
0231	<RequestPayload>
0232	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0233	<AttributeName type="TextString" value="Name"/>
0234	<AttributeName type="TextString" value="Contact Information"/>
0235	</RequestPayload>
0236	</BatchItem>
0237	</RequestMessage>
0238	<ResponseMessage>
0239	<ResponseHeader>
0240	<ProtocolVersion>
0241	<ProtocolVersionMajor type="Integer" value="1"/>
0242	<ProtocolVersionMinor type="Integer" value="1"/>
0243	</ProtocolVersion>
0244	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0245	<BatchCount type="Integer" value="1"/>
0246	</ResponseHeader>
0247	<BatchItem>
0248	<Operation type="Enumeration" value="GetAttributes"/>
0249	<ResultStatus type="Enumeration" value="Success"/>
0250	<ResponsePayload>
0251	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0252	<Attribute>
0253	<AttributeName type="TextString" value="Name"/>
0254	<AttributeValue>
0255	<NameValue type="TextString" value="TC-314-11-key1"/>
0256	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0257	</AttributeValue>
0258	</Attribute>
0259	<Attribute>
0260	<AttributeName type="TextString" value="Contact
	Information"/>
0261	<AttributeValue type="TextString" value="Foo"/>
0262	</Attribute>
0263	</ResponsePayload>
0264	</BatchItem>
0265	</ResponseMessage>
	# TIME 5
0266	<RequestMessage>
0267	<RequestHeader>
0268	<ProtocolVersion>
0269	<ProtocolVersionMajor type="Integer" value="1"/>
0270	<ProtocolVersionMinor type="Integer" value="1"/>
0271	</ProtocolVersion>
0272	<BatchCount type="Integer" value="2"/>
0273	</RequestHeader>
0274	<BatchItem>

0275	<Operation type="Enumeration" value="AddAttribute"/>
0276	<UniqueBatchItemID type="ByteString" value="32d84369c120488e"/>
0277	<RequestPayload>
0278	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0279	<Attribute>
0280	<AttributeName type="TextString" value="x-attribute1"/>
0281	<AttributeValue type="TextString" value="Value1"/>
0282	</Attribute>
0283	</RequestPayload>
0284	</BatchItem>
0285	<BatchItem>
0286	<Operation type="Enumeration" value="AddAttribute"/>
0287	<UniqueBatchItemID type="ByteString" value="519cf4f0eclac13f"/>
0288	<RequestPayload>
0289	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0290	<Attribute>
0291	<AttributeName type="TextString" value="x-attribute2"/>
0292	<AttributeValue type="TextString" value="Value2"/>
0293	</Attribute>
0294	</RequestPayload>
0295	</BatchItem>
0296	</RequestMessage>
0297	<ResponseMessage>
0298	<ResponseHeader>
0299	<ProtocolVersion>
0300	<ProtocolVersionMajor type="Integer" value="1"/>
0301	<ProtocolVersionMinor type="Integer" value="1"/>
0302	</ProtocolVersion>
0303	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0304	<BatchCount type="Integer" value="2"/>
0305	</ResponseHeader>
0306	<BatchItem>
0307	<Operation type="Enumeration" value="AddAttribute"/>
0308	<UniqueBatchItemID type="ByteString" value="32d84369c120488e"/>
0309	<ResultStatus type="Enumeration" value="Success"/>
0310	<ResponsePayload>
0311	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0312	<Attribute>
0313	<AttributeName type="TextString" value="x-attribute1"/>
0314	<AttributeValue type="TextString" value="Value1"/>
0315	</Attribute>
0316	</ResponsePayload>
0317	</BatchItem>
0318	<BatchItem>
0319	<Operation type="Enumeration" value="AddAttribute"/>
0320	<UniqueBatchItemID type="ByteString" value="519cf4f0eclac13f"/>
0321	<ResultStatus type="Enumeration" value="Success"/>
0322	<ResponsePayload>
0323	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0324	<Attribute>
0325	<AttributeName type="TextString" value="x-attribute2"/>
0326	<AttributeValue type="TextString" value="Value2"/>
0327	</Attribute>

0328	</ResponsePayload>
0329	</BatchItem>
0330	</ResponseMessage>
# TIME 6	
0331	<RequestMessage>
0332	<RequestHeader>
0333	<ProtocolVersion>
0334	<ProtocolVersionMajor type="Integer" value="1"/>
0335	<ProtocolVersionMinor type="Integer" value="1"/>
0336	</ProtocolVersion>
0337	<BatchCount type="Integer" value="2"/>
0338	</RequestHeader>
0339	<BatchItem>
0340	<Operation type="Enumeration" value="ModifyAttribute"/>
0341	<UniqueBatchItemID type="ByteString" value="fce08e45995686b6"/>
0342	<RequestPayload>
0343	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0344	<Attribute>
0345	<AttributeName type="TextString" value="x-attribute1"/>
0346	<AttributeValue type="TextString" value="ModifiedValue1"/>
0347	</Attribute>
0348	</RequestPayload>
0349	</BatchItem>
0350	<BatchItem>
0351	<Operation type="Enumeration" value="ModifyAttribute"/>
0352	<UniqueBatchItemID type="ByteString" value="dc2bfda88f39f5fc"/>
0353	<RequestPayload>
0354	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0355	<Attribute>
0356	<AttributeName type="TextString" value="x-attribute2"/>
0357	<AttributeValue type="TextString" value="ModifiedValue2"/>
0358	</Attribute>
0359	</RequestPayload>
0360	</BatchItem>
0361	</RequestMessage>
0362	<ResponseMessage>
0363	<ResponseHeader>
0364	<ProtocolVersion>
0365	<ProtocolVersionMajor type="Integer" value="1"/>
0366	<ProtocolVersionMinor type="Integer" value="1"/>
0367	</ProtocolVersion>
0368	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0369	<BatchCount type="Integer" value="2"/>
0370	</ResponseHeader>
0371	<BatchItem>
0372	<Operation type="Enumeration" value="ModifyAttribute"/>
0373	<UniqueBatchItemID type="ByteString" value="fce08e45995686b6"/>
0374	<ResultStatus type="Enumeration" value="Success"/>
0375	<ResponsePayload>
0376	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0377	<Attribute>
0378	<AttributeName type="TextString" value="x-attribute1"/>
0379	<AttributeValue type="TextString" value="ModifiedValue1"/>
0380	</Attribute>

0381	</ResponsePayload>
0382	</BatchItem>
0383	<BatchItem>
0384	<Operation type="Enumeration" value="ModifyAttribute"/>
0385	<UniqueBatchItemID type="ByteString" value="dc2bfda88f39f5fc"/>
0386	<ResultStatus type="Enumeration" value="Success"/>
0387	<ResponsePayload>
0388	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0389	<Attribute>
0390	<AttributeName type="TextString" value="x-attribute2"/>
0391	<AttributeValue type="TextString" value="ModifiedValue2"/>
0392	</Attribute>
0393	</ResponsePayload>
0394	</BatchItem>
0395	</ResponseMessage>
# TIME 7	
0396	<RequestMessage>
0397	<RequestHeader>
0398	<ProtocolVersion>
0399	<ProtocolVersionMajor type="Integer" value="1"/>
0400	<ProtocolVersionMinor type="Integer" value="1"/>
0401	</ProtocolVersion>
0402	<BatchCount type="Integer" value="2"/>
0403	</RequestHeader>
0404	<BatchItem>
0405	<Operation type="Enumeration" value="DeleteAttribute"/>
0406	<UniqueBatchItemID type="ByteString" value="ba8d4889753b7414"/>
0407	<RequestPayload>
0408	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0409	<AttributeName type="TextString" value="x-attribute1"/>
0410	</RequestPayload>
0411	</BatchItem>
0412	<BatchItem>
0413	<Operation type="Enumeration" value="DeleteAttribute"/>
0414	<UniqueBatchItemID type="ByteString" value="88fa2f142c615edb"/>
0415	<RequestPayload>
0416	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0417	<AttributeName type="TextString" value="x-attribute2"/>
0418	</RequestPayload>
0419	</BatchItem>
0420	</RequestMessage>
0421	<ResponseMessage>
0422	<ResponseHeader>
0423	<ProtocolVersion>
0424	<ProtocolVersionMajor type="Integer" value="1"/>
0425	<ProtocolVersionMinor type="Integer" value="1"/>
0426	</ProtocolVersion>
0427	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0428	<BatchCount type="Integer" value="2"/>
0429	</ResponseHeader>
0430	<BatchItem>
0431	<Operation type="Enumeration" value="DeleteAttribute"/>
0432	<UniqueBatchItemID type="ByteString" value="ba8d4889753b7414"/>
0433	<ResultStatus type="Enumeration" value="Success"/>

0434	<ResponsePayload>
0435	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0436	<Attribute>
0437	<AttributeName type="TextString" value="x-attribute1"/>
0438	<AttributeValue type="TextString" value="ModifiedValue1"/>
0439	</Attribute>
0440	</ResponsePayload>
0441	</BatchItem>
0442	<BatchItem>
0443	<Operation type="Enumeration" value="DeleteAttribute"/>
0444	<UniqueBatchItemID type="ByteString" value="88fa2f142c615edb"/>
0445	<ResultStatus type="Enumeration" value="Success"/>
0446	<ResponsePayload>
0447	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0448	<Attribute>
0449	<AttributeName type="TextString" value="x-attribute2"/>
0450	<AttributeValue type="TextString" value="ModifiedValue2"/>
0451	</Attribute>
0452	</ResponsePayload>
0453	</BatchItem>
0454	</ResponseMessage>
	# TIME 8
0455	<RequestMessage>
0456	<RequestHeader>
0457	<ProtocolVersion>
0458	<ProtocolVersionMajor type="Integer" value="1"/>
0459	<ProtocolVersionMinor type="Integer" value="1"/>
0460	</ProtocolVersion>
0461	<BatchCount type="Integer" value="1"/>
0462	</RequestHeader>
0463	<BatchItem>
0464	<Operation type="Enumeration" value="Destroy"/>
0465	<RequestPayload>
0466	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0467	</RequestPayload>
0468	</BatchItem>
0469	</RequestMessage>
0470	<ResponseMessage>
0471	<ResponseHeader>
0472	<ProtocolVersion>
0473	<ProtocolVersionMajor type="Integer" value="1"/>
0474	<ProtocolVersionMinor type="Integer" value="1"/>
0475	</ProtocolVersion>
0476	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0477	<BatchCount type="Integer" value="1"/>
0478	</ResponseHeader>
0479	<BatchItem>
0480	<Operation type="Enumeration" value="Destroy"/>
0481	<ResultStatus type="Enumeration" value="Success"/>
0482	<ResponsePayload>
0483	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0484	</ResponsePayload>
0485	</BatchItem>

0486	</ResponseMessage>
	# TIME 9
0487	<RequestMessage>
0488	<RequestHeader>
0489	<ProtocolVersion>
0490	<ProtocolVersionMajor type="Integer" value="1"/>
0491	<ProtocolVersionMinor type="Integer" value="1"/>
0492	</ProtocolVersion>
0493	<BatchCount type="Integer" value="1"/>
0494	</RequestHeader>
0495	<BatchItem>
0496	<Operation type="Enumeration" value="Get"/>
0497	<RequestPayload>
0498	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0499	</RequestPayload>
0500	</BatchItem>
0501	</RequestMessage>
0502	<ResponseMessage>
0503	<ResponseHeader>
0504	<ProtocolVersion>
0505	<ProtocolVersionMajor type="Integer" value="1"/>
0506	<ProtocolVersionMinor type="Integer" value="1"/>
0507	</ProtocolVersion>
0508	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0509	<BatchCount type="Integer" value="1"/>
0510	</ResponseHeader>
0511	<BatchItem>
0512	<Operation type="Enumeration" value="Get"/>
0513	<ResultStatus type="Enumeration" value="OperationFailed"/>
0514	<ResultReason type="Enumeration" value="ItemNotFound"/>
0515	<ResultMessage type="TextString" value="No Cryptographic Object
	found with given Unique Identifier"/>
0516	</BatchItem>
0517	</ResponseMessage>
	# TIME 10
0518	<RequestMessage>
0519	<RequestHeader>
0520	<ProtocolVersion>
0521	<ProtocolVersionMajor type="Integer" value="1"/>
0522	<ProtocolVersionMinor type="Integer" value="1"/>
0523	</ProtocolVersion>
0524	<BatchCount type="Integer" value="1"/>
0525	</RequestHeader>
0526	<BatchItem>
0527	<Operation type="Enumeration" value="Destroy"/>
0528	<RequestPayload>
0529	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0530	</RequestPayload>
0531	</BatchItem>
0532	</RequestMessage>
0533	<ResponseMessage>
0534	<ResponseHeader>
0535	<ProtocolVersion>
0536	<ProtocolVersionMajor type="Integer" value="1"/>

0537	<ProtocolVersionMinor type="Integer" value="1"/>
0538	</ProtocolVersion>
0539	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0540	<BatchCount type="Integer" value="1"/>
0541	</ResponseHeader>
0542	<BatchItem>
0543	<Operation type="Enumeration" value="Destroy"/>
0544	<ResultStatus type="Enumeration" value="Success"/>
0545	<ResponsePayload>
0546	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0547	</ResponsePayload>
0548	</BatchItem>
0549	</ResponseMessage>
# TIME 11	
0550	<RequestMessage>
0551	<RequestHeader>
0552	<ProtocolVersion>
0553	<ProtocolVersionMajor type="Integer" value="1"/>
0554	<ProtocolVersionMinor type="Integer" value="1"/>
0555	</ProtocolVersion>
0556	<BatchCount type="Integer" value="1"/>
0557	</RequestHeader>
0558	<BatchItem>
0559	<Operation type="Enumeration" value="Get"/>
0560	<RequestPayload>
0561	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0562	</RequestPayload>
0563	</BatchItem>
0564	</RequestMessage>
0565	<ResponseMessage>
0566	<ResponseHeader>
0567	<ProtocolVersion>
0568	<ProtocolVersionMajor type="Integer" value="1"/>
0569	<ProtocolVersionMinor type="Integer" value="1"/>
0570	</ProtocolVersion>
0571	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0572	<BatchCount type="Integer" value="1"/>
0573	</ResponseHeader>
0574	<BatchItem>
0575	<Operation type="Enumeration" value="Get"/>
0576	<ResultStatus type="Enumeration" value="OperationFailed"/>
0577	<ResultReason type="Enumeration" value="ItemNotFound"/>
0578	<ResultMessage type="TextString" value="No Cryptographic Object
	found with given Unique Identifier"/>
0579	</BatchItem>
0580	</ResponseMessage>

349

350 2.2.5 TC-315-11 - Register / Destroy Secret Data

351 In this test case the client issues a Register request containing a Secret Data object, whereby the
352 server registers the object and returns the Unique Identifier. To clean up, the client then
353 performs a Destroy

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SecretData"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Verify"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-315-11"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<SecretData>
0024	<SecretDataType type="Enumeration" value="Password"/>
0025	<KeyBlock>
0026	<KeyFormatType type="Enumeration" value="Opaque"/>
0027	<KeyValue>
0028	<KeyMaterial type="ByteString" value="53656372657450617373776f7264"/>
0029	</KeyValue>
0030	</KeyBlock>
0031	</SecretData>
0032	</RequestPayload>
0033	</BatchItem>
0034	</RequestMessage>
0035	<ResponseMessage>
0036	<ResponseHeader>
0037	<ProtocolVersion>
0038	<ProtocolVersionMajor type="Integer" value="1"/>
0039	<ProtocolVersionMinor type="Integer" value="1"/>
0040	</ProtocolVersion>
0041	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0042	<BatchCount type="Integer" value="1"/>
0043	</ResponseHeader>
0044	<BatchItem>
0045	<Operation type="Enumeration" value="Register"/>
0046	<ResultStatus type="Enumeration" value="Success"/>
0047	<ResponsePayload>
0048	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0049	</ResponsePayload>
0050	</BatchItem>
0051	</ResponseMessage>
	# TIME 1
0052	<RequestMessage>

0053	<RequestHeader>
0054	<ProtocolVersion>
0055	<ProtocolVersionMajor type="Integer" value="1"/>
0056	<ProtocolVersionMinor type="Integer" value="1"/>
0057	</ProtocolVersion>
0058	<BatchCount type="Integer" value="1"/>
0059	</RequestHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="Destroy"/>
0062	<RequestPayload>
0063	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0064	</RequestPayload>
0065	</BatchItem>
0066	</RequestMessage>
0067	<ResponseMessage>
0068	<ResponseHeader>
0069	<ProtocolVersion>
0070	<ProtocolVersionMajor type="Integer" value="1"/>
0071	<ProtocolVersionMinor type="Integer" value="1"/>
0072	</ProtocolVersion>
0073	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0074	<BatchCount type="Integer" value="1"/>
0075	</ResponseHeader>
0076	<BatchItem>
0077	<Operation type="Enumeration" value="Destroy"/>
0078	<ResultStatus type="Enumeration" value="Success"/>
0079	<ResponsePayload>
0080	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0081	</ResponsePayload>
0082	</BatchItem>
0083	</ResponseMessage>

354

355 2.2.6 TC-32-11 - Asynchronous Locate

356 This test case tests the asynchronous capabilities of KMIP using the Locate operation. A key is
357 created and then a Locate request is sent containing the Name of the created key and with the
358 message header Asynchronous Indicator-field set to True. If the server returns an asynchronous
359 response to the Locate, the client then polls the server until the operation is ready. If the server
360 responded asynchronously, a subsequent Locate operation that is also handled asynchronously
361 is then Canceled, before the key is finally destroyed.

362 This test case shows the use of two clients with the same assumptions as in the test case
363 described in Section . Since the client is unable to force the server to respond asynchronously, it
364 is possible for a server to respond synchronously to the requests issued at times 1 and 4, in
365 which case the expected response are the ones shown at times 2 and 5, respectively. In the case
366 of the server not responding asynchronously to the Locate requests, the client is permitted to
367 skip the requests illustrated at time 7 and 8.

	# TIME 0
0001	<RequestMessage>

0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Length"/>
0022	<AttributeValue type="Integer" value="128"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Name"/>
0026	<AttributeValue>
0027	<NameValue type="TextString" value="TC-32-12-key1"/>
0028	<NameType type="Enumeration"
0029	value="UninterpretedTextString"/>
0030	</AttributeValue>
0031	</Attribute>
0032	<Attribute>
0033	<AttributeName type="TextString" value="Cryptographic
0034	Usage Mask"/>
0035	<AttributeValue type="Integer" value="Encrypt"/>
0036	</Attribute>
0037	<Attribute>
0038	<AttributeName type="TextString" value="Object Group"/>
0039	<AttributeValue type="TextString" value="Group1"/>
0040	</Attribute>
0041	</TemplateAttribute>
0042	</RequestPayload>
0043	</BatchItem>
0044	</RequestMessage>
0045	<ResponseMessage>
0046	<ResponseHeader>
0047	<ProtocolVersion>
0048	<ProtocolVersionMajor type="Integer" value="1"/>
0049	<ProtocolVersionMinor type="Integer" value="1"/>
0050	</ProtocolVersion>
0051	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0052	<BatchCount type="Integer" value="1"/>
0053	</ResponseHeader>
0054	<BatchItem>
0055	<Operation type="Enumeration" value="Create"/>
0056	<ResultStatus type="Enumeration" value="Success"/>
0057	<ResponsePayload>
0058	<ObjectType type="Enumeration" value="SymmetricKey"/>

0055	<UniqueIdentifier type="TextString"
0056	value="\$UNIQUE_IDENTIFIER_0"/>
0057	</ResponsePayload>
0058	</BatchItem>
	</ResponseMessage>
	# TIME 1
0059	<RequestMessage>
0060	<RequestHeader>
0061	<ProtocolVersion>
0062	<ProtocolVersionMajor type="Integer" value="1"/>
0063	<ProtocolVersionMinor type="Integer" value="1"/>
0064	</ProtocolVersion>
0065	<AsynchronousIndicator type="Boolean" value="true"/>
0066	<BatchCount type="Integer" value="1"/>
0067	</RequestHeader>
0068	<BatchItem>
0069	<Operation type="Enumeration" value="Locate"/>
0070	<RequestPayload>
0071	<Attribute>
0072	<AttributeName type="TextString" value="Object Type"/>
0073	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0074	</Attribute>
0075	<Attribute>
0076	<AttributeName type="TextString" value="Name"/>
0077	<AttributeValue>
0078	<NameValue type="TextString" value="TC-32-12-key1"/>
0079	<NameType type="Enumeration"
0080	value="UninterpretedTextString"/>
0081	</AttributeValue>
0082	</Attribute>
0083	</RequestPayload>
0084	</BatchItem>
0085	</RequestMessage>
0086	<ResponseMessage>
0087	<ResponseHeader>
0088	<ProtocolVersion>
0089	<ProtocolVersionMajor type="Integer" value="1"/>
0090	<ProtocolVersionMinor type="Integer" value="1"/>
0091	</ProtocolVersion>
0092	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0093	<BatchCount type="Integer" value="1"/>
0094	</ResponseHeader>
0095	<BatchItem>
0096	<Operation type="Enumeration" value="Locate"/>
0097	<ResultStatus type="Enumeration" value="OperationPending"/>
0098	<AsynchronousCorrelationValue type="ByteString"
0099	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
	</BatchItem>
	</ResponseMessage>
	# TIME 2
0100	<RequestMessage>
0101	<RequestHeader>
0102	<ProtocolVersion>
0103	<ProtocolVersionMajor type="Integer" value="1"/>
0104	<ProtocolVersionMinor type="Integer" value="1"/>
0105	</ProtocolVersion>

0106	<BatchCount type="Integer" value="1"/>
0107	</RequestHeader>
0108	<BatchItem>
0109	<Operation type="Enumeration" value="Poll"/>
0110	<RequestPayload>
0111	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0112	</RequestPayload>
0113	</BatchItem>
0114	</RequestMessage>
0115	<ResponseMessage>
0116	<ResponseHeader>
0117	<ProtocolVersion>
0118	<ProtocolVersionMajor type="Integer" value="1"/>
0119	<ProtocolVersionMinor type="Integer" value="1"/>
0120	</ProtocolVersion>
0121	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0122	<BatchCount type="Integer" value="1"/>
0123	</ResponseHeader>
0124	<BatchItem>
0125	<Operation type="Enumeration" value="Locate"/>
0126	<ResultStatus type="Enumeration" value="Success"/>
0127	<ResponsePayload>
0128	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0129	</ResponsePayload>
0130	</BatchItem>
0131	</ResponseMessage>
	# TIME 3
0132	<RequestMessage>
0133	<RequestHeader>
0134	<ProtocolVersion>
0135	<ProtocolVersionMajor type="Integer" value="1"/>
0136	<ProtocolVersionMinor type="Integer" value="1"/>
0137	</ProtocolVersion>
0138	<BatchCount type="Integer" value="1"/>
0139	</RequestHeader>
0140	<BatchItem>
0141	<Operation type="Enumeration" value="Get"/>
0142	<RequestPayload>
0143	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0144	</RequestPayload>
0145	</BatchItem>
0146	</RequestMessage>
0147	<ResponseMessage>
0148	<ResponseHeader>
0149	<ProtocolVersion>
0150	<ProtocolVersionMajor type="Integer" value="1"/>
0151	<ProtocolVersionMinor type="Integer" value="1"/>
0152	</ProtocolVersion>
0153	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0154	<BatchCount type="Integer" value="1"/>
0155	</ResponseHeader>
0156	<BatchItem>
0157	<Operation type="Enumeration" value="Get"/>

0158	<ResultStatus type="Enumeration" value="Success"/>
0159	<ResponsePayload>
0160	<ObjectType type="Enumeration" value="SymmetricKey"/>
0161	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0162	<SymmetricKey>
0163	<KeyBlock>
0164	<KeyFormatType type="Enumeration" value="Raw"/>
0165	<KeyValue>
0166	<KeyMaterial type="ByteString"
	value="cc9e3b20f5c4fc4d1298f68d0b7de65b"/>
0167	</KeyValue>
0168	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0169	<CryptographicLength type="Integer" value="128"/>
0170	</KeyBlock>
0171	</SymmetricKey>
0172	</ResponsePayload>
0173	</BatchItem>
0174	</ResponseMessage>
	# TIME 4
0175	<RequestMessage>
0176	<RequestHeader>
0177	<ProtocolVersion>
0178	<ProtocolVersionMajor type="Integer" value="1"/>
0179	<ProtocolVersionMinor type="Integer" value="1"/>
0180	</ProtocolVersion>
0181	<AsynchronousIndicator type="Boolean" value="true"/>
0182	<BatchCount type="Integer" value="1"/>
0183	</RequestHeader>
0184	<BatchItem>
0185	<Operation type="Enumeration" value="Locate"/>
0186	<RequestPayload>
0187	<Attribute>
0188	<AttributeName type="TextString" value="Object Type"/>
0189	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0190	</Attribute>
0191	<Attribute>
0192	<AttributeName type="TextString" value="Object Group"/>
0193	<AttributeValue type="TextString" value="Group1"/>
0194	</Attribute>
0195	</RequestPayload>
0196	</BatchItem>
0197	</RequestMessage>
0198	<ResponseMessage>
0199	<ResponseHeader>
0200	<ProtocolVersion>
0201	<ProtocolVersionMajor type="Integer" value="1"/>
0202	<ProtocolVersionMinor type="Integer" value="1"/>
0203	</ProtocolVersion>
0204	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0205	<BatchCount type="Integer" value="1"/>
0206	</ResponseHeader>
0207	<BatchItem>
0208	<Operation type="Enumeration" value="Locate"/>
0209	<ResultStatus type="Enumeration" value="OperationPending"/>
0210	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>

0211	</BatchItem>
0212	</ResponseMessage>
0213	# TIME 5
0213	<RequestMessage>
0214	<RequestHeader>
0215	<ProtocolVersion>
0216	<ProtocolVersionMajor type="Integer" value="1"/>
0217	<ProtocolVersionMinor type="Integer" value="1"/>
0218	</ProtocolVersion>
0219	<BatchCount type="Integer" value="1"/>
0220	</RequestHeader>
0221	<BatchItem>
0222	<Operation type="Enumeration" value="Poll"/>
0223	<RequestPayload>
0224	<AsynchronousCorrelationValue type="ByteString" value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0225	</RequestPayload>
0226	</BatchItem>
0227	</RequestMessage>
0228	<ResponseMessage>
0229	<ResponseHeader>
0230	<ProtocolVersion>
0231	<ProtocolVersionMajor type="Integer" value="1"/>
0232	<ProtocolVersionMinor type="Integer" value="1"/>
0233	</ProtocolVersion>
0234	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0235	<BatchCount type="Integer" value="1"/>
0236	</ResponseHeader>
0237	<BatchItem>
0238	<Operation type="Enumeration" value="Locate"/>
0239	<ResultStatus type="Enumeration" value="Success"/>
0240	<ResponsePayload>
0241	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0242	</ResponsePayload>
0243	</BatchItem>
0244	</ResponseMessage>
0245	# TIME 6
0245	<RequestMessage>
0246	<RequestHeader>
0247	<ProtocolVersion>
0248	<ProtocolVersionMajor type="Integer" value="1"/>
0249	<ProtocolVersionMinor type="Integer" value="1"/>
0250	</ProtocolVersion>
0251	<BatchCount type="Integer" value="1"/>
0252	</RequestHeader>
0253	<BatchItem>
0254	<Operation type="Enumeration" value="Get"/>
0255	<RequestPayload>
0256	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0257	</RequestPayload>
0258	</BatchItem>
0259	</RequestMessage>
0260	<ResponseMessage>
0261	<ResponseHeader>

0262	<ProtocolVersion>
0263	<ProtocolVersionMajor type="Integer" value="1"/>
0264	<ProtocolVersionMinor type="Integer" value="1"/>
0265	</ProtocolVersion>
0266	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0267	<BatchCount type="Integer" value="1"/>
0268	</ResponseHeader>
0269	<BatchItem>
0270	<Operation type="Enumeration" value="Get"/>
0271	<ResultStatus type="Enumeration" value="Success"/>
0272	<ResponsePayload>
0273	<ObjectType type="Enumeration" value="SymmetricKey"/>
0274	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0275	<SymmetricKey>
0276	<KeyBlock>
0277	<KeyFormatType type="Enumeration" value="Raw"/>
0278	<KeyValue>
0279	<KeyMaterial type="ByteString"
	value="cc9e3b20f5c4fc4d1298f68d0b7de65b"/>
0280	</KeyValue>
0281	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0282	<CryptographicLength type="Integer" value="128"/>
0283	</KeyBlock>
0284	</SymmetricKey>
0285	</ResponsePayload>
0286	</BatchItem>
0287	</ResponseMessage>
	# TIME 7
0288	<RequestMessage>
0289	<RequestHeader>
0290	<ProtocolVersion>
0291	<ProtocolVersionMajor type="Integer" value="1"/>
0292	<ProtocolVersionMinor type="Integer" value="1"/>
0293	</ProtocolVersion>
0294	<AsynchronousIndicator type="Boolean" value="true"/>
0295	<BatchCount type="Integer" value="1"/>
0296	</RequestHeader>
0297	<BatchItem>
0298	<Operation type="Enumeration" value="Locate"/>
0299	<RequestPayload>
0300	<Attribute>
0301	<AttributeName type="TextString" value="Object Type"/>
0302	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0303	</Attribute>
0304	<Attribute>
0305	<AttributeName type="TextString" value="Name"/>
0306	<AttributeValue>
0307	<NameValue type="TextString" value="TC-32-12-key1"/>
0308	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0309	</AttributeValue>
0310	</Attribute>
0311	</RequestPayload>
0312	</BatchItem>
0313	</RequestMessage>
0314	<ResponseMessage>

0315	<ResponseHeader>
0316	<ProtocolVersion>
0317	<ProtocolVersionMajor type="Integer" value="1"/>
0318	<ProtocolVersionMinor type="Integer" value="1"/>
0319	</ProtocolVersion>
0320	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0321	<BatchCount type="Integer" value="1"/>
0322	</ResponseHeader>
0323	<BatchItem>
0324	<Operation type="Enumeration" value="Locate"/>
0325	<ResultStatus type="Enumeration" value="OperationPending"/>
0326	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0327	</BatchItem>
0328	</ResponseMessage>
	# TIME 8
0329	<RequestMessage>
0330	<RequestHeader>
0331	<ProtocolVersion>
0332	<ProtocolVersionMajor type="Integer" value="1"/>
0333	<ProtocolVersionMinor type="Integer" value="1"/>
0334	</ProtocolVersion>
0335	<BatchCount type="Integer" value="1"/>
0336	</RequestHeader>
0337	<BatchItem>
0338	<Operation type="Enumeration" value="Cancel"/>
0339	<RequestPayload>
0340	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0341	</RequestPayload>
0342	</BatchItem>
0343	</RequestMessage>
0344	<ResponseMessage>
0345	<ResponseHeader>
0346	<ProtocolVersion>
0347	<ProtocolVersionMajor type="Integer" value="1"/>
0348	<ProtocolVersionMinor type="Integer" value="1"/>
0349	</ProtocolVersion>
0350	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0351	<BatchCount type="Integer" value="1"/>
0352	</ResponseHeader>
0353	<BatchItem>
0354	<Operation type="Enumeration" value="Cancel"/>
0355	<ResultStatus type="Enumeration" value="Success"/>
0356	<ResponsePayload>
0357	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0358	<CancellationResult type="Enumeration" value="Canceled"/>
0359	</ResponsePayload>
0360	</BatchItem>
0361	</ResponseMessage>
	# TIME 9
0362	<RequestMessage>
0363	<RequestHeader>
0364	<ProtocolVersion>
0365	<ProtocolVersionMajor type="Integer" value="1"/>

0366	<ProtocolVersionMinor type="Integer" value="1"/>
0367	</ProtocolVersion>
0368	<BatchCount type="Integer" value="1"/>
0369	</RequestHeader>
0370	<BatchItem>
0371	<Operation type="Enumeration" value="Destroy"/>
0372	<RequestPayload>
0373	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0374	</RequestPayload>
0375	</BatchItem>
0376	</RequestMessage>
0377	<ResponseMessage>
0378	<ResponseHeader>
0379	<ProtocolVersion>
0380	<ProtocolVersionMajor type="Integer" value="1"/>
0381	<ProtocolVersionMinor type="Integer" value="1"/>
0382	</ProtocolVersion>
0383	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0384	<BatchCount type="Integer" value="1"/>
0385	</ResponseHeader>
0386	<BatchItem>
0387	<Operation type="Enumeration" value="Destroy"/>
0388	<ResultStatus type="Enumeration" value="Success"/>
0389	<ResponsePayload>
0390	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0391	</ResponsePayload>
0392	</BatchItem>
0393	</ResponseMessage>

368

369 2.2.7 TC-41-11 - Revoke Scenario

370 This test case tests the revocation aspect of the key life cycle support in KMIP. A key is created
371 and a Get Attribute for the State-attribute reveals that the key is in Pre-active state. The
372 Activation Date is then set, which changes the state to Active. The key is then revoked with a
373 revocation reason of Compromised and the state subsequently changed to Compromised, but
374 this does not stop a client from being able to add, modify and delete attributes or even get the
375 key (since we assume here that the out-of-band registration has been used to make the server
376 aware of the fact that the client is capable of interpreting the attributes of the key and
377 determining what it is allowed to do with the key). To clean up, the created key is finally
378 destroyed.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>

0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Length"/>
0022	<AttributeValue type="Integer" value="128"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Name"/>
0026	<AttributeValue>
0027	<NameValue type="TextString" value="TC-41-11-key1"/>
0028	<NameType type="Enumeration"
0029	value="UninterpretedTextString"/>
0030	</AttributeValue>
0031	</Attribute>
0032	<Attribute>
0033	<AttributeName type="TextString" value="Cryptographic
0034	Usage Mask"/>
0035	<AttributeValue type="Integer" value="Encrypt"/>
0036	</Attribute>
0037	</TemplateAttribute>
0038	</RequestPayload>
0039	</BatchItem>
0040	</RequestMessage>
0041	<ResponseMessage>
0042	<ResponseHeader>
0043	<ProtocolVersion>
0044	<ProtocolVersionMajor type="Integer" value="1"/>
0045	<ProtocolVersionMinor type="Integer" value="1"/>
0046	</ProtocolVersion>
0047	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0048	<BatchCount type="Integer" value="1"/>
0049	</ResponseHeader>
0050	<BatchItem>
0051	<Operation type="Enumeration" value="Create"/>
0052	<ResultStatus type="Enumeration" value="Success"/>
0053	<ResponsePayload>
0054	<ObjectType type="Enumeration" value="SymmetricKey"/>
0055	<UniqueIdentifier type="TextString"
0056	value="\$UNIQUE_IDENTIFIER_0"/>
0057	</ResponsePayload>
0058	</BatchItem>
0059	</ResponseMessage>
0060	# TIME 1
0061	<RequestMessage>
0062	<RequestHeader>
0063	<ProtocolVersion>
0064	<ProtocolVersionMajor type="Integer" value="1"/>
0065	<ProtocolVersionMinor type="Integer" value="1"/>
0066	</ProtocolVersion>

0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="GetAttributes"/>
0065	<RequestPayload>
0066	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0067	<AttributeName type="TextString" value="State"/>
0068	</RequestPayload>
0069	</BatchItem>
0070	</RequestMessage>
0071	<ResponseMessage>
0072	<ResponseHeader>
0073	<ProtocolVersion>
0074	<ProtocolVersionMajor type="Integer" value="1"/>
0075	<ProtocolVersionMinor type="Integer" value="1"/>
0076	</ProtocolVersion>
0077	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0078	<BatchCount type="Integer" value="1"/>
0079	</ResponseHeader>
0080	<BatchItem>
0081	<Operation type="Enumeration" value="GetAttributes"/>
0082	<ResultStatus type="Enumeration" value="Success"/>
0083	<ResponsePayload>
0084	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0085	<Attribute>
0086	<AttributeName type="TextString" value="State"/>
0087	<AttributeValue type="Enumeration" value="PreActive"/>
0088	</Attribute>
0089	</ResponsePayload>
0090	</BatchItem>
0091	</ResponseMessage>
	# TIME 2
0092	<RequestMessage>
0093	<RequestHeader>
0094	<ProtocolVersion>
0095	<ProtocolVersionMajor type="Integer" value="1"/>
0096	<ProtocolVersionMinor type="Integer" value="1"/>
0097	</ProtocolVersion>
0098	<BatchCount type="Integer" value="1"/>
0099	</RequestHeader>
0100	<BatchItem>
0101	<Operation type="Enumeration" value="Activate"/>
0102	<RequestPayload>
0103	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0104	</RequestPayload>
0105	</BatchItem>
0106	</RequestMessage>
0107	<ResponseMessage>
0108	<ResponseHeader>
0109	<ProtocolVersion>
0110	<ProtocolVersionMajor type="Integer" value="1"/>
0111	<ProtocolVersionMinor type="Integer" value="1"/>
0112	</ProtocolVersion>

0113	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0114	<BatchCount type="Integer" value="1"/>
0115	</ResponseHeader>
0116	<BatchItem>
0117	<Operation type="Enumeration" value="Activate"/>
0118	<ResultStatus type="Enumeration" value="Success"/>
0119	<ResponsePayload>
0120	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0121	</ResponsePayload>
0122	</BatchItem>
0123	</ResponseMessage>
	# TIME 3
0124	<RequestMessage>
0125	<RequestHeader>
0126	<ProtocolVersion>
0127	<ProtocolVersionMajor type="Integer" value="1"/>
0128	<ProtocolVersionMinor type="Integer" value="1"/>
0129	</ProtocolVersion>
0130	<BatchCount type="Integer" value="1"/>
0131	</RequestHeader>
0132	<BatchItem>
0133	<Operation type="Enumeration" value="GetAttributes"/>
0134	<RequestPayload>
0135	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0136	<AttributeName type="TextString" value="State"/>
0137	</RequestPayload>
0138	</BatchItem>
0139	</RequestMessage>
0140	<ResponseMessage>
0141	<ResponseHeader>
0142	<ProtocolVersion>
0143	<ProtocolVersionMajor type="Integer" value="1"/>
0144	<ProtocolVersionMinor type="Integer" value="1"/>
0145	</ProtocolVersion>
0146	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0147	<BatchCount type="Integer" value="1"/>
0148	</ResponseHeader>
0149	<BatchItem>
0150	<Operation type="Enumeration" value="GetAttributes"/>
0151	<ResultStatus type="Enumeration" value="Success"/>
0152	<ResponsePayload>
0153	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0154	<Attribute>
0155	<AttributeName type="TextString" value="State"/>
0156	<AttributeValue type="Enumeration" value="Active"/>
0157	</Attribute>
0158	</ResponsePayload>
0159	</BatchItem>
0160	</ResponseMessage>
	# TIME 4
0161	<RequestMessage>
0162	<RequestHeader>
0163	<ProtocolVersion>

0164	<ProtocolVersionMajor type="Integer" value="1"/>
0165	<ProtocolVersionMinor type="Integer" value="1"/>
0166	</ProtocolVersion>
0167	<BatchCount type="Integer" value="1"/>
0168	</RequestHeader>
0169	<BatchItem>
0170	<Operation type="Enumeration" value="Locate"/>
0171	<RequestPayload>
0172	<Attribute>
0173	<AttributeName type="TextString" value="Object Type"/>
0174	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0175	</Attribute>
0176	<Attribute>
0177	<AttributeName type="TextString" value="Name"/>
0178	<AttributeValue>
0179	<NameValue type="TextString" value="TC-41-11-key1"/>
0180	<NameType type="Enumeration"
0181	value="UninterpretedTextString"/>
0182	</AttributeValue>
0183	</Attribute>
0184	</RequestPayload>
0185	</BatchItem>
0186	</RequestMessage>
0187	<ResponseMessage>
0188	<ResponseHeader>
0189	<ProtocolVersion>
0190	<ProtocolVersionMajor type="Integer" value="1"/>
0191	<ProtocolVersionMinor type="Integer" value="1"/>
0192	</ProtocolVersion>
0193	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0194	<BatchCount type="Integer" value="1"/>
0195	</ResponseHeader>
0196	<BatchItem>
0197	<Operation type="Enumeration" value="Locate"/>
0198	<ResultStatus type="Enumeration" value="Success"/>
0199	<ResponsePayload>
0200	<UniqueIdentifier type="TextString"
0201	value="\$UNIQUE_IDENTIFIER_0"/>
0202	</ResponsePayload>
0203	</BatchItem>
0204	</ResponseMessage>
0205	# TIME 5
0206	<RequestMessage>
0207	<RequestHeader>
0208	<ProtocolVersion>
0209	<ProtocolVersionMajor type="Integer" value="1"/>
0210	<ProtocolVersionMinor type="Integer" value="1"/>
0211	</ProtocolVersion>
0212	<BatchCount type="Integer" value="1"/>
0213	</RequestHeader>
0214	<BatchItem>
0215	<Operation type="Enumeration" value="Get"/>
0216	<RequestPayload>
	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
	</RequestPayload>
	</BatchItem>

0217	</RequestMessage>
0218	<ResponseMessage>
0219	<ResponseHeader>
0220	<ProtocolVersion>
0221	<ProtocolVersionMajor type="Integer" value="1"/>
0222	<ProtocolVersionMinor type="Integer" value="1"/>
0223	</ProtocolVersion>
0224	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0225	<BatchCount type="Integer" value="1"/>
0226	</ResponseHeader>
0227	<BatchItem>
0228	<Operation type="Enumeration" value="Get"/>
0229	<ResultStatus type="Enumeration" value="Success"/>
0230	<ResponsePayload>
0231	<ObjectType type="Enumeration" value="SymmetricKey"/>
0232	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0233	<SymmetricKey>
0234	<KeyBlock>
0235	<KeyFormatType type="Enumeration" value="Raw"/>
0236	<KeyValue>
0237	<KeyMaterial type="ByteString"
	value="9c7d7c4fd2076f1909a6ba4342cab1de"/>
0238	</KeyMaterial>
0239	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0240	<CryptographicLength type="Integer" value="128"/>
0241	</KeyBlock>
0242	</SymmetricKey>
0243	</ResponsePayload>
0244	</BatchItem>
0245	</ResponseMessage>
	# TIME 6
0246	<RequestMessage>
0247	<RequestHeader>
0248	<ProtocolVersion>
0249	<ProtocolVersionMajor type="Integer" value="1"/>
0250	<ProtocolVersionMinor type="Integer" value="1"/>
0251	</ProtocolVersion>
0252	<BatchCount type="Integer" value="1"/>
0253	</RequestHeader>
0254	<BatchItem>
0255	<Operation type="Enumeration" value="Revoke"/>
0256	<RequestPayload>
0257	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0258	<RevocationReason>
0259	<RevocationReasonCode type="Enumeration"
	value="KeyCompromise"/>
0260	</RevocationReason>
0261	<CompromiseOccurrenceDate type="DateTime" value="1970-01-
	01T00:06:00+00:00"/>
0262	</RequestPayload>
0263	</BatchItem>
0264	</RequestMessage>
0265	<ResponseMessage>
0266	<ResponseHeader>

0267	<ProtocolVersion>
0268	<ProtocolVersionMajor type="Integer" value="1"/>
0269	<ProtocolVersionMinor type="Integer" value="1"/>
0270	</ProtocolVersion>
0271	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0272	<BatchCount type="Integer" value="1"/>
0273	</ResponseHeader>
0274	<BatchItem>
0275	<Operation type="Enumeration" value="Revoke"/>
0276	<ResultStatus type="Enumeration" value="Success"/>
0277	<ResponsePayload>
0278	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0279	</ResponsePayload>
0280	</BatchItem>
0281	</ResponseMessage>
# TIME 7	
0282	<RequestMessage>
0283	<RequestHeader>
0284	<ProtocolVersion>
0285	<ProtocolVersionMajor type="Integer" value="1"/>
0286	<ProtocolVersionMinor type="Integer" value="1"/>
0287	</ProtocolVersion>
0288	<BatchCount type="Integer" value="1"/>
0289	</RequestHeader>
0290	<BatchItem>
0291	<Operation type="Enumeration" value="GetAttributes"/>
0292	<RequestPayload>
0293	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0294	<AttributeName type="TextString" value="State"/>
0295	</RequestPayload>
0296	</BatchItem>
0297	</RequestMessage>
0298	<ResponseMessage>
0299	<ResponseHeader>
0300	<ProtocolVersion>
0301	<ProtocolVersionMajor type="Integer" value="1"/>
0302	<ProtocolVersionMinor type="Integer" value="1"/>
0303	</ProtocolVersion>
0304	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0305	<BatchCount type="Integer" value="1"/>
0306	</ResponseHeader>
0307	<BatchItem>
0308	<Operation type="Enumeration" value="GetAttributes"/>
0309	<ResultStatus type="Enumeration" value="Success"/>
0310	<ResponsePayload>
0311	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0312	<Attribute>
0313	<AttributeName type="TextString" value="State"/>
0314	<AttributeValue type="Enumeration" value="Compromised"/>
0315	</Attribute>
0316	</ResponsePayload>
0317	</BatchItem>
0318	</ResponseMessage>

0319 0320 0321 0322 0323 0324 0325 0326 0327 0328 0329 0330 0331 0332 0333	<pre> # TIME 8 <RequestMessage> <RequestHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="1"/> </ProtocolVersion> <BatchCount type="Integer" value="1"/> </RequestHeader> <BatchItem> <Operation type="Enumeration" value="GetAttributeList"/> <RequestPayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/> </RequestPayload> </BatchItem> </RequestMessage> </pre>
0334 0335 0336 0337 0338 0339 0340 0341 0342 0343 0344 0345 0346 0347 0348 0349 0350 0351 0352 0353 0354 0355 0356 0357 0358 0359 0360 0361 0362 0363 0364 0365 0366	<pre> <ResponseMessage> <ResponseHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="1"/> </ProtocolVersion> <TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/> <BatchCount type="Integer" value="1"/> </ResponseHeader> <BatchItem> <Operation type="Enumeration" value="GetAttributeList"/> <ResultStatus type="Enumeration" value="Success"/> <ResponsePayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/> <AttributeName type="TextString" value="Cryptographic Length"/> <AttributeName type="TextString" value="Cryptographic Algorithm"/> <AttributeName type="TextString" value="State"/> <AttributeName type="TextString" value="Compromise Occurrence Date"/> <AttributeName type="TextString" value="Compromise Date"/> <AttributeName type="TextString" value="Digest"/> <AttributeName type="TextString" value="Lease Time"/> <AttributeName type="TextString" value="Initial Date"/> <AttributeName type="TextString" value="Activation Date"/> <AttributeName type="TextString" value="Revocation Reason"/> <AttributeName type="TextString" value="Unique Identifier"/> <AttributeName type="TextString" value="Name"/> <AttributeName type="TextString" value="Cryptographic Usage Mask"/> <AttributeName type="TextString" value="Object Type"/> <AttributeName type="TextString" value="Last Change Date"/> <AttributeName type="TextString" value="Fresh"/> </ResponsePayload> </BatchItem> </ResponseMessage> </pre>
0367	<pre> # TIME 9 <RequestMessage> </pre>

0368	<RequestHeader>
0369	<ProtocolVersion>
0370	<ProtocolVersionMajor type="Integer" value="1"/>
0371	<ProtocolVersionMinor type="Integer" value="1"/>
0372	</ProtocolVersion>
0373	<BatchCount type="Integer" value="1"/>
0374	</RequestHeader>
0375	<BatchItem>
0376	<Operation type="Enumeration" value="GetAttributes"/>
0377	<RequestPayload>
0378	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0379	<AttributeName type="TextString" value="State"/>
0380	</RequestPayload>
0381	</BatchItem>
0382	</RequestMessage>
0383	<ResponseMessage>
0384	<ResponseHeader>
0385	<ProtocolVersion>
0386	<ProtocolVersionMajor type="Integer" value="1"/>
0387	<ProtocolVersionMinor type="Integer" value="1"/>
0388	</ProtocolVersion>
0389	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0390	<BatchCount type="Integer" value="1"/>
0391	</ResponseHeader>
0392	<BatchItem>
0393	<Operation type="Enumeration" value="GetAttributes"/>
0394	<ResultStatus type="Enumeration" value="Success"/>
0395	<ResponsePayload>
0396	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0397	<Attribute>
0398	<AttributeName type="TextString" value="State"/>
0399	<AttributeValue type="Enumeration" value="Compromised"/>
0400	</Attribute>
0401	</ResponsePayload>
0402	</BatchItem>
0403	</ResponseMessage>
	# TIME 10
0404	<RequestMessage>
0405	<RequestHeader>
0406	<ProtocolVersion>
0407	<ProtocolVersionMajor type="Integer" value="1"/>
0408	<ProtocolVersionMinor type="Integer" value="1"/>
0409	</ProtocolVersion>
0410	<BatchCount type="Integer" value="2"/>
0411	</RequestHeader>
0412	<BatchItem>
0413	<Operation type="Enumeration" value="AddAttribute"/>
0414	<UniqueBatchItemID type="ByteString" value="23a177faa569463c"/>
0415	<RequestPayload>
0416	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0417	<Attribute>
0418	<AttributeName type="TextString" value="x-attribute1"/>
0419	<AttributeValue type="TextString" value="Value1"/>
0420	</Attribute>

0421	</RequestPayload>
0422	</BatchItem>
0423	<BatchItem>
0424	<Operation type="Enumeration" value="AddAttribute"/>
0425	<UniqueBatchItemID type="ByteString" value="9b898dc0577f8080"/>
0426	<RequestPayload>
0427	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0428	<Attribute>
0429	<AttributeName type="TextString" value="x-attribute2"/>
0430	<AttributeValue type="TextString" value="Value2"/>
0431	</Attribute>
0432	</RequestPayload>
0433	</BatchItem>
0434	</RequestMessage>
0435	<ResponseMessage>
0436	<ResponseHeader>
0437	<ProtocolVersion>
0438	<ProtocolVersionMajor type="Integer" value="1"/>
0439	<ProtocolVersionMinor type="Integer" value="1"/>
0440	</ProtocolVersion>
0441	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0442	<BatchCount type="Integer" value="2"/>
0443	</ResponseHeader>
0444	<BatchItem>
0445	<Operation type="Enumeration" value="AddAttribute"/>
0446	<UniqueBatchItemID type="ByteString" value="23a177faa569463c"/>
0447	<ResultStatus type="Enumeration" value="Success"/>
0448	<ResponsePayload>
0449	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0450	<Attribute>
0451	<AttributeName type="TextString" value="x-attribute1"/>
0452	<AttributeValue type="TextString" value="Value1"/>
0453	</Attribute>
0454	</ResponsePayload>
0455	</BatchItem>
0456	<BatchItem>
0457	<Operation type="Enumeration" value="AddAttribute"/>
0458	<UniqueBatchItemID type="ByteString" value="9b898dc0577f8080"/>
0459	<ResultStatus type="Enumeration" value="Success"/>
0460	<ResponsePayload>
0461	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0462	<Attribute>
0463	<AttributeName type="TextString" value="x-attribute2"/>
0464	<AttributeValue type="TextString" value="Value2"/>
0465	</Attribute>
0466	</ResponsePayload>
0467	</BatchItem>
0468	</ResponseMessage>
	# TIME 11
0469	<RequestMessage>
0470	<RequestHeader>
0471	<ProtocolVersion>
0472	<ProtocolVersionMajor type="Integer" value="1"/>
0473	<ProtocolVersionMinor type="Integer" value="1"/>

0474	</ProtocolVersion>
0475	<BatchCount type="Integer" value="2"/>
0476	</RequestHeader>
0477	<BatchItem>
0478	<Operation type="Enumeration" value="ModifyAttribute"/>
0479	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0480	<RequestPayload>
0481	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0482	<Attribute>
0483	<AttributeName type="TextString" value="x-attribute1"/>
0484	<AttributeValue type="TextString" value="ModifiedValue1"/>
0485	</Attribute>
0486	</RequestPayload>
0487	</BatchItem>
0488	<BatchItem>
0489	<Operation type="Enumeration" value="ModifyAttribute"/>
0490	<UniqueBatchItemID type="ByteString" value="33f55c8d7e6cafbf"/>
0491	<RequestPayload>
0492	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0493	<Attribute>
0494	<AttributeName type="TextString" value="x-attribute2"/>
0495	<AttributeValue type="TextString" value="ModifiedValue2"/>
0496	</Attribute>
0497	</RequestPayload>
0498	</BatchItem>
0499	</RequestMessage>
0500	<ResponseMessage>
0501	<ResponseHeader>
0502	<ProtocolVersion>
0503	<ProtocolVersionMajor type="Integer" value="1"/>
0504	<ProtocolVersionMinor type="Integer" value="1"/>
0505	</ProtocolVersion>
0506	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0507	<BatchCount type="Integer" value="2"/>
0508	</ResponseHeader>
0509	<BatchItem>
0510	<Operation type="Enumeration" value="ModifyAttribute"/>
0511	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0512	<ResultStatus type="Enumeration" value="Success"/>
0513	<ResponsePayload>
0514	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0515	<Attribute>
0516	<AttributeName type="TextString" value="x-attribute1"/>
0517	<AttributeValue type="TextString" value="ModifiedValue1"/>
0518	</Attribute>
0519	</ResponsePayload>
0520	</BatchItem>
0521	<BatchItem>
0522	<Operation type="Enumeration" value="ModifyAttribute"/>
0523	<UniqueBatchItemID type="ByteString" value="33f55c8d7e6cafbf"/>
0524	<ResultStatus type="Enumeration" value="Success"/>
0525	<ResponsePayload>
0526	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0527	<Attribute>
0528	<AttributeName type="TextString" value="x-attribute2"/>
0529	<AttributeValue type="TextString" value="ModifiedValue2"/>
0530	</Attribute>
0531	</ResponsePayload>
0532	</BatchItem>
0533	</ResponseMessage>
# TIME 12	
0534	<RequestMessage>
0535	<RequestHeader>
0536	<ProtocolVersion>
0537	<ProtocolVersionMajor type="Integer" value="1"/>
0538	<ProtocolVersionMinor type="Integer" value="1"/>
0539	</ProtocolVersion>
0540	<BatchCount type="Integer" value="2"/>
0541	</RequestHeader>
0542	<BatchItem>
0543	<Operation type="Enumeration" value="DeleteAttribute"/>
0544	<UniqueBatchItemID type="ByteString" value="a3eb249b495e8ad2"/>
0545	<RequestPayload>
0546	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0547	<AttributeName type="TextString" value="x-attribute1"/>
0548	</RequestPayload>
0549	</BatchItem>
0550	<BatchItem>
0551	<Operation type="Enumeration" value="DeleteAttribute"/>
0552	<UniqueBatchItemID type="ByteString" value="c1fe7b3b4c977730"/>
0553	<RequestPayload>
0554	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0555	<AttributeName type="TextString" value="x-attribute2"/>
0556	</RequestPayload>
0557	</BatchItem>
0558	</RequestMessage>
0559	<ResponseMessage>
0560	<ResponseHeader>
0561	<ProtocolVersion>
0562	<ProtocolVersionMajor type="Integer" value="1"/>
0563	<ProtocolVersionMinor type="Integer" value="1"/>
0564	</ProtocolVersion>
0565	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0566	<BatchCount type="Integer" value="2"/>
0567	</ResponseHeader>
0568	<BatchItem>
0569	<Operation type="Enumeration" value="DeleteAttribute"/>
0570	<UniqueBatchItemID type="ByteString" value="a3eb249b495e8ad2"/>
0571	<ResultStatus type="Enumeration" value="Success"/>
0572	<ResponsePayload>
0573	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0574	<Attribute>
0575	<AttributeName type="TextString" value="x-attribute1"/>
0576	<AttributeValue type="TextString" value="ModifiedValue1"/>
0577	</Attribute>
0578	</ResponsePayload>
0579	</BatchItem>

0580	<BatchItem>
0581	<Operation type="Enumeration" value="DeleteAttribute"/>
0582	<UniqueBatchItemID type="ByteString" value="c1fe7b3b4c977730"/>
0583	<ResultStatus type="Enumeration" value="Success"/>
0584	<ResponsePayload>
0585	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0586	<Attribute>
0587	<AttributeName type="TextString" value="x-attribute2"/>
0588	<AttributeValue type="TextString" value="ModifiedValue2"/>
0589	</Attribute>
0590	</ResponsePayload>
0591	</BatchItem>
0592	</ResponseMessage>
# TIME 13	
0593	<RequestMessage>
0594	<RequestHeader>
0595	<ProtocolVersion>
0596	<ProtocolVersionMajor type="Integer" value="1"/>
0597	<ProtocolVersionMinor type="Integer" value="1"/>
0598	</ProtocolVersion>
0599	<BatchCount type="Integer" value="1"/>
0600	</RequestHeader>
0601	<BatchItem>
0602	<Operation type="Enumeration" value="Get"/>
0603	<RequestPayload>
0604	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0605	</RequestPayload>
0606	</BatchItem>
0607	</RequestMessage>
0608	<ResponseMessage>
0609	<ResponseHeader>
0610	<ProtocolVersion>
0611	<ProtocolVersionMajor type="Integer" value="1"/>
0612	<ProtocolVersionMinor type="Integer" value="1"/>
0613	</ProtocolVersion>
0614	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0615	<BatchCount type="Integer" value="1"/>
0616	</ResponseHeader>
0617	<BatchItem>
0618	<Operation type="Enumeration" value="Get"/>
0619	<ResultStatus type="Enumeration" value="Success"/>
0620	<ResponsePayload>
0621	<ObjectType type="Enumeration" value="SymmetricKey"/>
0622	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0623	<SymmetricKey>
0624	<KeyBlock>
0625	<KeyFormatType type="Enumeration" value="Raw"/>
0626	<KeyValue>
0627	<KeyMaterial type="ByteString"
	value="9c7d7c4fd2076f1909a6ba4342cab1de"/>
0628	</KeyValue>
0629	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0630	<CryptographicLength type="Integer" value="128"/>
0631	</KeyBlock>

0632	</SymmetricKey>
0633	</ResponsePayload>
0634	</BatchItem>
0635	</ResponseMessage>
# TIME 14	
0636	<RequestMessage>
0637	<RequestHeader>
0638	<ProtocolVersion>
0639	<ProtocolVersionMajor type="Integer" value="1"/>
0640	<ProtocolVersionMinor type="Integer" value="1"/>
0641	</ProtocolVersion>
0642	<BatchCount type="Integer" value="1"/>
0643	</RequestHeader>
0644	<BatchItem>
0645	<Operation type="Enumeration" value="Destroy"/>
0646	<RequestPayload>
0647	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0648	</RequestPayload>
0649	</BatchItem>
0650	</RequestMessage>
0651	<ResponseMessage>
0652	<ResponseHeader>
0653	<ProtocolVersion>
0654	<ProtocolVersionMajor type="Integer" value="1"/>
0655	<ProtocolVersionMinor type="Integer" value="1"/>
0656	</ProtocolVersion>
0657	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0658	<BatchCount type="Integer" value="1"/>
0659	</ResponseHeader>
0660	<BatchItem>
0661	<Operation type="Enumeration" value="Destroy"/>
0662	<ResultStatus type="Enumeration" value="Success"/>
0663	<ResponsePayload>
0664	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0665	</ResponsePayload>
0666	</BatchItem>
0667	</ResponseMessage>

379

380 2.2.8 TC-51-11 - Get Usage Allocation Scenario

381 This test case tests the usage management functionality of KMIP. A key is created and the
382 Activation Date and Protect Stop Date attributes are set in such a way as to allow the Get Usage
383 Allocation operation to be performed. The value of the Usage Limits attribute is set to 1000
384 bytes, and two subsequent requests for 500 bytes succeed (one of them also verifying the
385 amount that can be received using the Check operation), while a third fails since the usage
386 allocation has been used up. The key is finally revoked and destroyed. This test case shows the
387 use of multiple clients (Client-A, Client-B and Client-C).

# TIME 0	
# [Client-A]	
0001	<RequestMessage>

0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Length"/>
0022	<AttributeValue type="Integer" value="128"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Name"/>
0026	<AttributeValue>
0027	<NameValue type="TextString" value="TC-51-11-key1"/>
0028	<NameType type="Enumeration"
0029	value="UninterpretedTextString"/>
0030	</AttributeValue>
0031	</Attribute>
0032	<Attribute>
0033	<AttributeName type="TextString" value="Cryptographic
0034	Usage Mask"/>
0035	<AttributeValue type="Integer" value="Encrypt"/>
0036	</Attribute>
0037	</TemplateAttribute>
0038	</RequestPayload>
0039	</BatchItem>
0040	</RequestMessage>
0041	<ResponseMessage>
0042	<ResponseHeader>
0043	<ProtocolVersion>
0044	<ProtocolVersionMajor type="Integer" value="1"/>
0045	<ProtocolVersionMinor type="Integer" value="1"/>
0046	</ProtocolVersion>
0047	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0048	<BatchCount type="Integer" value="1"/>
0049	</ResponseHeader>
0050	<BatchItem>
0051	<Operation type="Enumeration" value="Create"/>
0052	<ResultStatus type="Enumeration" value="Success"/>
0053	<ResponsePayload>
0054	<ObjectType type="Enumeration" value="SymmetricKey"/>
0055	<UniqueIdentifier type="TextString"
0056	value="\$UNIQUE_IDENTIFIER_0"/>
0057	</ResponsePayload>
0058	</BatchItem>

0054	</ResponseMessage>
	# TIME 1
	# [Client-A]
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="1"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="2"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="AddAttribute"/>
0065	<UniqueBatchItemID type="ByteString" value="369f6802ee57532b"/>
0066	<RequestPayload>
0067	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0068	<Attribute>
0069	<AttributeName type="TextString" value="Activation Date"/>
0070	<AttributeValue type="DateTime" value="\$NOW-3600"/>
0071	</Attribute>
0072	</RequestPayload>
0073	</BatchItem>
0074	<BatchItem>
0075	<Operation type="Enumeration" value="AddAttribute"/>
0076	<UniqueBatchItemID type="ByteString" value="b7ca806e52825bf4"/>
0077	<RequestPayload>
0078	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0079	<Attribute>
0080	<AttributeName type="TextString" value="Protect Stop Date"/>
0081	<AttributeValue type="DateTime" value="\$NOW+600"/>
0082	</Attribute>
0083	</RequestPayload>
0084	</BatchItem>
0085	</RequestMessage>
0086	<ResponseMessage>
0087	<ResponseHeader>
0088	<ProtocolVersion>
0089	<ProtocolVersionMajor type="Integer" value="1"/>
0090	<ProtocolVersionMinor type="Integer" value="1"/>
0091	</ProtocolVersion>
0092	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0093	<BatchCount type="Integer" value="2"/>
0094	</ResponseHeader>
0095	<BatchItem>
0096	<Operation type="Enumeration" value="AddAttribute"/>
0097	<UniqueBatchItemID type="ByteString" value="369f6802ee57532b"/>
0098	<ResultStatus type="Enumeration" value="Success"/>
0099	<ResponsePayload>
0100	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0101	<Attribute>
0102	<AttributeName type="TextString" value="Activation Date"/>
0103	<AttributeValue type="DateTime" value="\$NOW-3600"/>
0104	</Attribute>
0105	</ResponsePayload>

0106	</BatchItem>
0107	<BatchItem>
0108	<Operation type="Enumeration" value="AddAttribute"/>
0109	<UniqueBatchItemID type="ByteString" value="b7ca806e52825bf4"/>
0110	<ResultStatus type="Enumeration" value="Success"/>
0111	<ResponsePayload>
0112	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0113	<Attribute>
0114	<AttributeName type="TextString" value="Protect Stop Date"/>
0115	<AttributeValue type="DateTime" value="\$NOW+600"/>
0116	</Attribute>
0117	</ResponsePayload>
0118	</BatchItem>
0119	</ResponseMessage>
	# TIME 2
	# [Client-A]
0120	<RequestMessage>
0121	<RequestHeader>
0122	<ProtocolVersion>
0123	<ProtocolVersionMajor type="Integer" value="1"/>
0124	<ProtocolVersionMinor type="Integer" value="1"/>
0125	</ProtocolVersion>
0126	<BatchCount type="Integer" value="1"/>
0127	</RequestHeader>
0128	<BatchItem>
0129	<Operation type="Enumeration" value="AddAttribute"/>
0130	<RequestPayload>
0131	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0132	<Attribute>
0133	<AttributeName type="TextString" value="Usage Limits"/>
0134	<AttributeValue>
0135	<UsageLimitsTotal type="LongInteger" value="1000"/>
0136	<UsageLimitsUnit type="Enumeration" value="Byte"/>
0137	</AttributeValue>
0138	</Attribute>
0139	</RequestPayload>
0140	</BatchItem>
0141	</RequestMessage>
0142	<ResponseMessage>
0143	<ResponseHeader>
0144	<ProtocolVersion>
0145	<ProtocolVersionMajor type="Integer" value="1"/>
0146	<ProtocolVersionMinor type="Integer" value="1"/>
0147	</ProtocolVersion>
0148	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0149	<BatchCount type="Integer" value="1"/>
0150	</ResponseHeader>
0151	<BatchItem>
0152	<Operation type="Enumeration" value="AddAttribute"/>
0153	<ResultStatus type="Enumeration" value="Success"/>
0154	<ResponsePayload>
0155	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0156	<Attribute>
0157	<AttributeName type="TextString" value="Usage Limits"/>

0158	<AttributeValue>
0159	<UsageLimitsTotal type="LongInteger" value="1000"/>
0160	<UsageLimitsCount type="LongInteger" value="1000"/>
0161	<UsageLimitsUnit type="Enumeration" value="Byte"/>
0162	</AttributeValue>
0163	</Attribute>
0164	</ResponsePayload>
0165	</BatchItem>
0166	</ResponseMessage>
	# TIME 3
	# [Client-B]
0167	<RequestMessage>
0168	<RequestHeader>
0169	<ProtocolVersion>
0170	<ProtocolVersionMajor type="Integer" value="1"/>
0171	<ProtocolVersionMinor type="Integer" value="1"/>
0172	</ProtocolVersion>
0173	<BatchCount type="Integer" value="1"/>
0174	</RequestHeader>
0175	<BatchItem>
0176	<Operation type="Enumeration" value="Locate"/>
0177	<RequestPayload>
0178	<Attribute>
0179	<AttributeName type="TextString" value="Object Type"/>
0180	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0181	</Attribute>
0182	<Attribute>
0183	<AttributeName type="TextString" value="Name"/>
0184	<AttributeValue>
0185	<NameValue type="TextString" value="TC-51-11-key1"/>
0186	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0187	</AttributeValue>
0188	</Attribute>
0189	</RequestPayload>
0190	</BatchItem>
0191	</RequestMessage>
0192	<ResponseMessage>
0193	<ResponseHeader>
0194	<ProtocolVersion>
0195	<ProtocolVersionMajor type="Integer" value="1"/>
0196	<ProtocolVersionMinor type="Integer" value="1"/>
0197	</ProtocolVersion>
0198	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0199	<BatchCount type="Integer" value="1"/>
0200	</ResponseHeader>
0201	<BatchItem>
0202	<Operation type="Enumeration" value="Locate"/>
0203	<ResultStatus type="Enumeration" value="Success"/>
0204	<ResponsePayload>
0205	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0206	</ResponsePayload>
0207	</BatchItem>
0208	</ResponseMessage>
	# TIME 4

0209	# [Client-B]
0210	<RequestMessage>
0211	<RequestHeader>
0212	<ProtocolVersion>
0213	<ProtocolVersionMajor type="Integer" value="1"/>
0214	<ProtocolVersionMinor type="Integer" value="1"/>
0215	</ProtocolVersion>
0216	<BatchCount type="Integer" value="1"/>
0217	</RequestHeader>
0218	<BatchItem>
0219	<Operation type="Enumeration" value="Get"/>
0220	<RequestPayload>
0221	<UniqueIdentifier type="TextString"
0222	value="\$UNIQUE_IDENTIFIER_0"/>
0223	</RequestPayload>
0224	</BatchItem>
0225	</RequestMessage>
0226	<ResponseMessage>
0227	<ResponseHeader>
0228	<ProtocolVersion>
0229	<ProtocolVersionMajor type="Integer" value="1"/>
0230	<ProtocolVersionMinor type="Integer" value="1"/>
0231	</ProtocolVersion>
0232	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0233	<BatchCount type="Integer" value="1"/>
0234	</ResponseHeader>
0235	<BatchItem>
0236	<Operation type="Enumeration" value="Get"/>
0237	<ResultStatus type="Enumeration" value="Success"/>
0238	<ResponsePayload>
0239	<ObjectType type="Enumeration" value="SymmetricKey"/>
0240	<UniqueIdentifier type="TextString"
0241	value="\$UNIQUE_IDENTIFIER_0"/>
0242	<SymmetricKey>
0243	<KeyBlock>
0244	<KeyFormatType type="Enumeration" value="Raw"/>
0245	<KeyValue>
0246	<KeyMaterial type="ByteString"
0247	value="50f31013c771af4448110f695efa9ec7"/>
0248	</KeyValue>
0249	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0250	<CryptographicLength type="Integer" value="128"/>
0251	</KeyBlock>
0252	</SymmetricKey>
0253	</ResponsePayload>
0254	</BatchItem>
0255	</ResponseMessage>
0256	# TIME 5
0257	# [Client-B]
0258	<RequestMessage>
0259	<RequestHeader>
0260	<ProtocolVersion>
0261	<ProtocolVersionMajor type="Integer" value="1"/>
0262	<ProtocolVersionMinor type="Integer" value="1"/>
0263	</ProtocolVersion>
0264	<BatchOrderOption type="Boolean" value="true"/>
0265	<BatchCount type="Integer" value="2"/>

0260	</RequestHeader>
0261	<BatchItem>
0262	<Operation type="Enumeration" value="Check"/>
0263	<UniqueBatchItemID type="ByteString" value="d35a294f9425f06e"/>
0264	<RequestPayload>
0265	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0266	<UsageLimitsCount type="LongInteger" value="500"/>
0267	</RequestPayload>
0268	</BatchItem>
0269	<BatchItem>
0270	<Operation type="Enumeration" value="GetUsageAllocation"/>
0271	<UniqueBatchItemID type="ByteString" value="80454d8ce4f738fe"/>
0272	<RequestPayload>
0273	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0274	<UsageLimitsCount type="LongInteger" value="500"/>
0275	</RequestPayload>
0276	</BatchItem>
0277	</RequestMessage>
0278	<ResponseMessage>
0279	<ResponseHeader>
0280	<ProtocolVersion>
0281	<ProtocolVersionMajor type="Integer" value="1"/>
0282	<ProtocolVersionMinor type="Integer" value="1"/>
0283	</ProtocolVersion>
0284	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0285	<BatchCount type="Integer" value="2"/>
0286	</ResponseHeader>
0287	<BatchItem>
0288	<Operation type="Enumeration" value="Check"/>
0289	<UniqueBatchItemID type="ByteString" value="d35a294f9425f06e"/>
0290	<ResultStatus type="Enumeration" value="Success"/>
0291	<ResponsePayload>
0292	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0293	</ResponsePayload>
0294	</BatchItem>
0295	<BatchItem>
0296	<Operation type="Enumeration" value="GetUsageAllocation"/>
0297	<UniqueBatchItemID type="ByteString" value="80454d8ce4f738fe"/>
0298	<ResultStatus type="Enumeration" value="Success"/>
0299	<ResponsePayload>
0300	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0301	</ResponsePayload>
0302	</BatchItem>
0303	</ResponseMessage>
	# TIME 6
	# [Client-A]
0304	<RequestMessage>
0305	<RequestHeader>
0306	<ProtocolVersion>
0307	<ProtocolVersionMajor type="Integer" value="1"/>
0308	<ProtocolVersionMinor type="Integer" value="1"/>
0309	</ProtocolVersion>
0310	<BatchCount type="Integer" value="1"/>

0311	</RequestHeader>
0312	<BatchItem>
0313	<Operation type="Enumeration" value="GetUsageAllocation"/>
0314	<RequestPayload>
0315	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0316	<UsageLimitsCount type="LongInteger" value="500"/>
0317	</RequestPayload>
0318	</BatchItem>
0319	</RequestMessage>
0320	<ResponseMessage>
0321	<ResponseHeader>
0322	<ProtocolVersion>
0323	<ProtocolVersionMajor type="Integer" value="1"/>
0324	<ProtocolVersionMinor type="Integer" value="1"/>
0325	</ProtocolVersion>
0326	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0327	<BatchCount type="Integer" value="1"/>
0328	</ResponseHeader>
0329	<BatchItem>
0330	<Operation type="Enumeration" value="GetUsageAllocation"/>
0331	<ResultStatus type="Enumeration" value="Success"/>
0332	<ResponsePayload>
0333	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0334	</ResponsePayload>
0335	</BatchItem>
0336	</ResponseMessage>
	# TIME 7
	# [Client-C]
0337	<RequestMessage>
0338	<RequestHeader>
0339	<ProtocolVersion>
0340	<ProtocolVersionMajor type="Integer" value="1"/>
0341	<ProtocolVersionMinor type="Integer" value="1"/>
0342	</ProtocolVersion>
0343	<BatchCount type="Integer" value="1"/>
0344	</RequestHeader>
0345	<BatchItem>
0346	<Operation type="Enumeration" value="Locate"/>
0347	<RequestPayload>
0348	<Attribute>
0349	<AttributeName type="TextString" value="Object Type"/>
0350	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0351	</Attribute>
0352	<Attribute>
0353	<AttributeName type="TextString" value="Name"/>
0354	<AttributeValue>
0355	<NameValue type="TextString" value="TC-51-11-key1"/>
0356	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0357	</AttributeValue>
0358	</Attribute>
0359	</RequestPayload>
0360	</BatchItem>
0361	</RequestMessage>

0362	<ResponseMessage>
0363	<ResponseHeader>
0364	<ProtocolVersion>
0365	<ProtocolVersionMajor type="Integer" value="1"/>
0366	<ProtocolVersionMinor type="Integer" value="1"/>
0367	</ProtocolVersion>
0368	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0369	<BatchCount type="Integer" value="1"/>
0370	</ResponseHeader>
0371	<BatchItem>
0372	<Operation type="Enumeration" value="Locate"/>
0373	<ResultStatus type="Enumeration" value="Success"/>
0374	<ResponsePayload>
0375	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0376	</ResponsePayload>
0377	</BatchItem>
0378	</ResponseMessage>
# TIME 8	
# [Client-C]	
0379	<RequestMessage>
0380	<RequestHeader>
0381	<ProtocolVersion>
0382	<ProtocolVersionMajor type="Integer" value="1"/>
0383	<ProtocolVersionMinor type="Integer" value="1"/>
0384	</ProtocolVersion>
0385	<BatchCount type="Integer" value="1"/>
0386	</RequestHeader>
0387	<BatchItem>
0388	<Operation type="Enumeration" value="Get"/>
0389	<RequestPayload>
0390	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0391	</RequestPayload>
0392	</BatchItem>
0393	</RequestMessage>
0394	<ResponseMessage>
0395	<ResponseHeader>
0396	<ProtocolVersion>
0397	<ProtocolVersionMajor type="Integer" value="1"/>
0398	<ProtocolVersionMinor type="Integer" value="1"/>
0399	</ProtocolVersion>
0400	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0401	<BatchCount type="Integer" value="1"/>
0402	</ResponseHeader>
0403	<BatchItem>
0404	<Operation type="Enumeration" value="Get"/>
0405	<ResultStatus type="Enumeration" value="Success"/>
0406	<ResponsePayload>
0407	<ObjectType type="Enumeration" value="SymmetricKey"/>
0408	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0409	<SymmetricKey>
0410	<KeyBlock>
0411	<KeyFormatType type="Enumeration" value="Raw"/>
0412	<KeyValue>
0413	<KeyMaterial type="ByteString"

0414	value="50f31013c771af4448110f695efa9ec7"/>
0415	</KeyValue>
0416	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0417	<CryptographicLength type="Integer" value="128"/>
0418	</KeyBlock>
0419	</SymmetricKey>
0420	</ResponsePayload>
0421	</BatchItem>
0422	</ResponseMessage>
0423	# TIME 9
0424	# [Client-C]
0425	<RequestMessage>
0426	<RequestHeader>
0427	<ProtocolVersion>
0428	<ProtocolVersionMajor type="Integer" value="1"/>
0429	<ProtocolVersionMinor type="Integer" value="1"/>
0430	</ProtocolVersion>
0431	<BatchCount type="Integer" value="1"/>
0432	</RequestHeader>
0433	<BatchItem>
0434	<Operation type="Enumeration" value="GetUsageAllocation"/>
0435	<RequestPayload>
0436	<UniqueIdentifier type="TextString"
0437	value="\$UNIQUE_IDENTIFIER_0"/>
0438	<UsageLimitsCount type="LongInteger" value="500"/>
0439	</RequestPayload>
0440	</BatchItem>
0441	</RequestMessage>
0442	<ResponseMessage>
0443	<ResponseHeader>
0444	<ProtocolVersion>
0445	<ProtocolVersionMajor type="Integer" value="1"/>
0446	<ProtocolVersionMinor type="Integer" value="1"/>
0447	</ProtocolVersion>
0448	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0449	<BatchCount type="Integer" value="1"/>
0450	</ResponseHeader>
0451	<BatchItem>
0452	<Operation type="Enumeration" value="GetUsageAllocation"/>
0453	<ResultStatus type="Enumeration" value="OperationFailed"/>
0454	<ResultReason type="Enumeration" value="PermissionDenied"/>
0455	<ResultMessage type="TextString" value="Unable to allocate
0456	requested amount"/>
0457	</BatchItem>
0458	</ResponseMessage>
0459	# TIME 10
0460	# [Client-A]
0461	<RequestMessage>
0462	<RequestHeader>
0463	<ProtocolVersion>
0464	<ProtocolVersionMajor type="Integer" value="1"/>
0465	<ProtocolVersionMinor type="Integer" value="1"/>
0466	</ProtocolVersion>
0467	<BatchOrderOption type="Boolean" value="true"/>
0468	<BatchCount type="Integer" value="2"/>
0469	</RequestHeader>

0463	<BatchItem>
0464	<Operation type="Enumeration" value="Revoke"/>
0465	<UniqueBatchItemID type="ByteString" value="79b998c5f29465f4"/>
0466	<RequestPayload>
0467	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0468	<RevocationReason>
0469	<RevocationReasonCode type="Enumeration"
	value="CessationOfOperation"/>
0470	</RevocationReason>
0471	</RequestPayload>
0472	</BatchItem>
0473	<BatchItem>
0474	<Operation type="Enumeration" value="Destroy"/>
0475	<UniqueBatchItemID type="ByteString" value="b0633f0e41187345"/>
0476	<RequestPayload>
0477	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0478	</RequestPayload>
0479	</BatchItem>
0480	</RequestMessage>
0481	<ResponseMessage>
0482	<ResponseHeader>
0483	<ProtocolVersion>
0484	<ProtocolVersionMajor type="Integer" value="1"/>
0485	<ProtocolVersionMinor type="Integer" value="1"/>
0486	</ProtocolVersion>
0487	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0488	<BatchCount type="Integer" value="2"/>
0489	</ResponseHeader>
0490	<BatchItem>
0491	<Operation type="Enumeration" value="Revoke"/>
0492	<UniqueBatchItemID type="ByteString" value="79b998c5f29465f4"/>
0493	<ResultStatus type="Enumeration" value="Success"/>
0494	<ResponsePayload>
0495	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0496	</ResponsePayload>
0497	</BatchItem>
0498	<BatchItem>
0499	<Operation type="Enumeration" value="Destroy"/>
0500	<UniqueBatchItemID type="ByteString" value="b0633f0e41187345"/>
0501	<ResultStatus type="Enumeration" value="Success"/>
0502	<ResponsePayload>
0503	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0504	</ResponsePayload>
0505	</BatchItem>
0506	</ResponseMessage>

388

389 2.2.9 TC-61-11 - Import of a Third-party Key

390 This test case tests the import of a foreign key using the Register operation. To validate that the
391 registered key is treated the same as a locally created key, an attribute is added to the key and
392 then modified. Finally, the key is destroyed.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Encrypt"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-61-11"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<SymmetricKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="Raw"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString" value="0123456789abcdef0123456789abcdef"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0030	<CryptographicLength type="Integer" value="128"/>
0031	</KeyBlock>
0032	</SymmetricKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="1"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1

0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="1"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="AddAttribute"/>
0063	<RequestPayload>
0064	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0065	<Attribute>
0066	<AttributeName type="TextString" value="x-provider"/>
0067	<AttributeValue type="TextString" value="unknown"/>
0068	</Attribute>
0069	</RequestPayload>
0070	</BatchItem>
0071	</RequestMessage>
0072	<ResponseMessage>
0073	<ResponseHeader>
0074	<ProtocolVersion>
0075	<ProtocolVersionMajor type="Integer" value="1"/>
0076	<ProtocolVersionMinor type="Integer" value="1"/>
0077	</ProtocolVersion>
0078	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0079	<BatchCount type="Integer" value="1"/>
0080	</ResponseHeader>
0081	<BatchItem>
0082	<Operation type="Enumeration" value="AddAttribute"/>
0083	<ResultStatus type="Enumeration" value="Success"/>
0084	<ResponsePayload>
0085	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0086	<Attribute>
0087	<AttributeName type="TextString" value="x-provider"/>
0088	<AttributeValue type="TextString" value="unknown"/>
0089	</Attribute>
0090	</ResponsePayload>
0091	</BatchItem>
0092	</ResponseMessage>
	# TIME 2
0093	<RequestMessage>
0094	<RequestHeader>
0095	<ProtocolVersion>
0096	<ProtocolVersionMajor type="Integer" value="1"/>
0097	<ProtocolVersionMinor type="Integer" value="1"/>
0098	</ProtocolVersion>
0099	<BatchCount type="Integer" value="1"/>
0100	</RequestHeader>
0101	<BatchItem>
0102	<Operation type="Enumeration" value="ModifyAttribute"/>
0103	<RequestPayload>
0104	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0105	<Attribute>

0106	<AttributeName type="TextString" value="x-provider"/>
0107	<AttributeValue type="TextString" value="third party"/>
0108	</Attribute>
0109	</RequestPayload>
0110	</BatchItem>
0111	</RequestMessage>
0112	<ResponseMessage>
0113	<ResponseHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="1"/>
0117	</ProtocolVersion>
0118	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0119	<BatchCount type="Integer" value="1"/>
0120	</ResponseHeader>
0121	<BatchItem>
0122	<Operation type="Enumeration" value="ModifyAttribute"/>
0123	<ResultStatus type="Enumeration" value="Success"/>
0124	<ResponsePayload>
0125	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0126	<Attribute>
0127	<AttributeName type="TextString" value="x-provider"/>
0128	<AttributeValue type="TextString" value="third party"/>
0129	</Attribute>
0130	</ResponsePayload>
0131	</BatchItem>
0132	</ResponseMessage>
	# TIME 3
0133	<RequestMessage>
0134	<RequestHeader>
0135	<ProtocolVersion>
0136	<ProtocolVersionMajor type="Integer" value="1"/>
0137	<ProtocolVersionMinor type="Integer" value="1"/>
0138	</ProtocolVersion>
0139	<BatchCount type="Integer" value="1"/>
0140	</RequestHeader>
0141	<BatchItem>
0142	<Operation type="Enumeration" value="Destroy"/>
0143	<RequestPayload>
0144	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0145	</RequestPayload>
0146	</BatchItem>
0147	</RequestMessage>
0148	<ResponseMessage>
0149	<ResponseHeader>
0150	<ProtocolVersion>
0151	<ProtocolVersionMajor type="Integer" value="1"/>
0152	<ProtocolVersionMinor type="Integer" value="1"/>
0153	</ProtocolVersion>
0154	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0155	<BatchCount type="Integer" value="1"/>
0156	</ResponseHeader>
0157	<BatchItem>
0158	<Operation type="Enumeration" value="Destroy"/>

0159	<ResultStatus type="Enumeration" value="Success"/>
0160	<ResponsePayload>
0161	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0162	</ResponsePayload>
0163	</BatchItem>
0164	</ResponseMessage>

393

394 2.2.10 TC-71-11 - Unrecognized Message Extension with Criticality Indicator
395 False

396 A create request is issued and the request contains a Message Extension with the Criticality
397 Indicator set to false. The server does not understand the extension, but since it is non-critical,
398 the create request is processed normally. Subsequently, the created key is deleted.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0016	<AttributeValue type="Integer" value="128"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0020	<AttributeValue type="Enumeration" value="AES"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="x-ID"/>
0028	<AttributeValue type="TextString" value="TC-71-11"/>
0029	</Attribute>
0030	</TemplateAttribute>
0031	</RequestPayload>
0032	<MessageExtension>
0033	<VendorIdentification type="TextString" value="Acme"/>
0034	<CriticalityIndicator type="Boolean" value="false"/>
0035	<VendorExtension>

0036	<TLV tag="0x540001" type="TextString" value="na"/>
0037	</VendorExtension>
0038	</MessageExtension>
0039	</BatchItem>
0040	</RequestMessage>
0041	<ResponseMessage>
0042	<ResponseHeader>
0043	<ProtocolVersion>
0044	<ProtocolVersionMajor type="Integer" value="1"/>
0045	<ProtocolVersionMinor type="Integer" value="1"/>
0046	</ProtocolVersion>
0047	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0048	<BatchCount type="Integer" value="1"/>
0049	</ResponseHeader>
0050	<BatchItem>
0051	<Operation type="Enumeration" value="Create"/>
0052	<ResultStatus type="Enumeration" value="Success"/>
0053	<ResponsePayload>
0054	<ObjectType type="Enumeration" value="SymmetricKey"/>
0055	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0056	</ResponsePayload>
0057	</BatchItem>
0058	</ResponseMessage>
0059	# TIME 1
0060	<RequestMessage>
0061	<RequestHeader>
0062	<ProtocolVersion>
0063	<ProtocolVersionMajor type="Integer" value="1"/>
0064	<ProtocolVersionMinor type="Integer" value="1"/>
0065	</ProtocolVersion>
0066	<BatchCount type="Integer" value="1"/>
0067	</RequestHeader>
0068	<BatchItem>
0069	<Operation type="Enumeration" value="Destroy"/>
0070	<RequestPayload>
0071	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0072	</RequestPayload>
0073	</BatchItem>
0074	</RequestMessage>
0075	<ResponseMessage>
0076	<ResponseHeader>
0077	<ProtocolVersion>
0078	<ProtocolVersionMajor type="Integer" value="1"/>
0079	<ProtocolVersionMinor type="Integer" value="1"/>
0080	</ProtocolVersion>
0081	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0082	<BatchCount type="Integer" value="1"/>
0083	</ResponseHeader>
0084	<BatchItem>
0085	<Operation type="Enumeration" value="Destroy"/>
0086	<ResultStatus type="Enumeration" value="Success"/>
0087	<ResponsePayload>
	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0088	</ResponsePayload>
0089	</BatchItem>
0090	</ResponseMessage>

399

400 2.2.11 TC-72-11 - Unrecognized Message Extension with Criticality Indicator 401 True

402 A create request is issued and the request contains a Message Extension with the Criticality
403 Indicator set to true. The server does not understand the extension, and since it is critical, the
404 create request fails and an error is returned.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Length"/>
0016	<AttributeValue type="Integer" value="128"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0020	<AttributeValue type="Enumeration" value="AES"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="x-ID"/>
0028	<AttributeValue type="TextString" value="TC-72-11"/>
0029	</Attribute>
0030	</TemplateAttribute>
0031	</RequestPayload>
0032	<MessageExtension>
0033	<VendorIdentification type="TextString" value="Acme"/>
0034	<CriticalityIndicator type="Boolean" value="true"/>
0035	<VendorExtension>
0036	<TLV tag="0x540001" type="TextString" value="na"/>
0037	</VendorExtension>
0038	</MessageExtension>
0039	</BatchItem>

```

0040 </RequestMessage>
0041 <ResponseMessage>
0042   <ResponseHeader>
0043     <ProtocolVersion>
0044       <ProtocolVersionMajor type="Integer" value="1"/>
0045       <ProtocolVersionMinor type="Integer" value="1"/>
0046     </ProtocolVersion>
0047     <TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0048     <BatchCount type="Integer" value="1"/>
0049   </ResponseHeader>
0050   <BatchItem>
0051     <Operation type="Enumeration" value="Create"/>
0052     <ResultStatus type="Enumeration" value="OperationFailed"/>
0053     <ResultReason type="Enumeration" value="FeatureNotSupported"/>
0054     <ResultMessage type="TextString" value="Critical Message
Extension not recognized"/>
0055   </BatchItem>
0056 </ResponseMessage>

```

405

406 2.2.12 TC-81-11 - Create a Key Pair

407 Create a new private/public key pair. Make sure they are linked correctly by issuing Locate
408 commands with the assigned Unique Identifiers. Finally delete both key halves.

```

# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="1"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="CreateKeyPair"/>
0011     <RequestPayload>
0012       <CommonTemplateAttribute>
0013         <Attribute>
0014           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0015           <AttributeValue type="Enumeration" value="RSA"/>
0016         </Attribute>
0017         <Attribute>
0018           <AttributeName type="TextString" value="Cryptographic
Length"/>
0019           <AttributeValue type="Integer" value="1024"/>
0020         </Attribute>
0021       </CommonTemplateAttribute>
0022       <PrivateKeyTemplateAttribute>
0023         <Attribute>
0024           <AttributeName type="TextString" value="Name"/>
0025           <AttributeValue>
0026             <NameValue type="TextString" value="TC-81-11-
privatekey1"/>
0027           <NameType type="Enumeration"

```

0028	value="UninterpretedTextString"/>
0029	</AttributeValue>
0030	</Attribute>
0031	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0032	<AttributeValue type="Integer" value="Sign"/>
0033	</Attribute>
0034	</PrivateKeyTemplateAttribute>
0035	<PublicKeyTemplateAttribute>
0036	<Attribute>
0037	<AttributeName type="TextString" value="Name"/>
0038	<AttributeValue>
0039	<NameValue type="TextString" value="TC-81-11-publickey1"/>
0040	<NameType type="Enumeration" value="UninterpretedTextString"/>
0041	</AttributeValue>
0042	</Attribute>
0043	<Attribute>
0044	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0045	<AttributeValue type="Integer" value="Verify"/>
0046	</Attribute>
0047	</PublicKeyTemplateAttribute>
0048	</RequestPayload>
0049	</BatchItem>
0050	</RequestMessage>
0051	<ResponseMessage>
0052	<ResponseHeader>
0053	<ProtocolVersion>
0054	<ProtocolVersionMajor type="Integer" value="1"/>
0055	<ProtocolVersionMinor type="Integer" value="1"/>
0056	</ProtocolVersion>
0057	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0058	<BatchCount type="Integer" value="1"/>
0059	</ResponseHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="CreateKeyPair"/>
0062	<ResultStatus type="Enumeration" value="Success"/>
0063	<ResponsePayload>
0064	<PrivateKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0065	<PublicKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
0069	# TIME 1 <RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="1"/>
0074	</ProtocolVersion>
0075	<BatchCount type="Integer" value="1"/>
0076	</RequestHeader>

0077	<BatchItem>
0078	<Operation type="Enumeration" value="Locate"/>
0079	<RequestPayload>
0080	<Attribute>
0081	<AttributeName type="TextString" value="Object Type"/>
0082	<AttributeValue type="Enumeration" value="PublicKey"/>
0083	</Attribute>
0084	<Attribute>
0085	<AttributeName type="TextString" value="Link"/>
0086	<AttributeValue>
0087	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0088	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0089	</AttributeValue>
0090	</Attribute>
0091	</RequestPayload>
0092	</BatchItem>
0093	</RequestMessage>
0094	<ResponseMessage>
0095	<ResponseHeader>
0096	<ProtocolVersion>
0097	<ProtocolVersionMajor type="Integer" value="1"/>
0098	<ProtocolVersionMinor type="Integer" value="1"/>
0099	</ProtocolVersion>
0100	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0101	<BatchCount type="Integer" value="1"/>
0102	</ResponseHeader>
0103	<BatchItem>
0104	<Operation type="Enumeration" value="Locate"/>
0105	<ResultStatus type="Enumeration" value="Success"/>
0106	<ResponsePayload>
0107	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0108	</ResponsePayload>
0109	</BatchItem>
0110	</ResponseMessage>
	# TIME 2
0111	<RequestMessage>
0112	<RequestHeader>
0113	<ProtocolVersion>
0114	<ProtocolVersionMajor type="Integer" value="1"/>
0115	<ProtocolVersionMinor type="Integer" value="1"/>
0116	</ProtocolVersion>
0117	<BatchCount type="Integer" value="1"/>
0118	</RequestHeader>
0119	<BatchItem>
0120	<Operation type="Enumeration" value="Locate"/>
0121	<RequestPayload>
0122	<Attribute>
0123	<AttributeName type="TextString" value="Object Type"/>
0124	<AttributeValue type="Enumeration" value="PrivateKey"/>
0125	</Attribute>
0126	<Attribute>
0127	<AttributeName type="TextString" value="Link"/>
0128	<AttributeValue>
0129	<LinkType type="Enumeration" value="PublicKeyLink"/>
0130	<LinkedObjectIdentifier type="TextString"

0131	value="\$UNIQUE_IDENTIFIER_1"/>
0132	</AttributeValue>
0133	</Attribute>
0134	</RequestPayload>
0135	</BatchItem>
0136	</RequestMessage>
0136	<ResponseMessage>
0137	<ResponseHeader>
0138	<ProtocolVersion>
0139	<ProtocolVersionMajor type="Integer" value="1"/>
0140	<ProtocolVersionMinor type="Integer" value="1"/>
0141	</ProtocolVersion>
0142	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0143	<BatchCount type="Integer" value="1"/>
0144	</ResponseHeader>
0145	<BatchItem>
0146	<Operation type="Enumeration" value="Locate"/>
0147	<ResultStatus type="Enumeration" value="Success"/>
0148	<ResponsePayload>
0149	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0150	</ResponsePayload>
0151	</BatchItem>
0152	</ResponseMessage>
0153	# TIME 3
0153	<RequestMessage>
0154	<RequestHeader>
0155	<ProtocolVersion>
0156	<ProtocolVersionMajor type="Integer" value="1"/>
0157	<ProtocolVersionMinor type="Integer" value="1"/>
0158	</ProtocolVersion>
0159	<BatchCount type="Integer" value="1"/>
0160	</RequestHeader>
0161	<BatchItem>
0162	<Operation type="Enumeration" value="Destroy"/>
0163	<RequestPayload>
0164	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0165	</RequestPayload>
0166	</BatchItem>
0167	</RequestMessage>
0168	<ResponseMessage>
0169	<ResponseHeader>
0170	<ProtocolVersion>
0171	<ProtocolVersionMajor type="Integer" value="1"/>
0172	<ProtocolVersionMinor type="Integer" value="1"/>
0173	</ProtocolVersion>
0174	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0175	<BatchCount type="Integer" value="1"/>
0176	</ResponseHeader>
0177	<BatchItem>
0178	<Operation type="Enumeration" value="Destroy"/>
0179	<ResultStatus type="Enumeration" value="Success"/>
0180	<ResponsePayload>
0181	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0182	</ResponsePayload>
0183	</BatchItem>
0184	</ResponseMessage>
# TIME 4	
0185	<RequestMessage>
0186	<RequestHeader>
0187	<ProtocolVersion>
0188	<ProtocolVersionMajor type="Integer" value="1"/>
0189	<ProtocolVersionMinor type="Integer" value="1"/>
0190	</ProtocolVersion>
0191	<BatchCount type="Integer" value="1"/>
0192	</RequestHeader>
0193	<BatchItem>
0194	<Operation type="Enumeration" value="Destroy"/>
0195	<RequestPayload>
0196	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0197	</RequestPayload>
0198	</BatchItem>
0199	</RequestMessage>
0200	<ResponseMessage>
0201	<ResponseHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="1"/>
0205	</ProtocolVersion>
0206	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0207	<BatchCount type="Integer" value="1"/>
0208	</ResponseHeader>
0209	<BatchItem>
0210	<Operation type="Enumeration" value="Destroy"/>
0211	<ResultStatus type="Enumeration" value="Success"/>
0212	<ResponsePayload>
0213	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0214	</ResponsePayload>
0215	</BatchItem>
0216	</ResponseMessage>

409

410 2.2.13 TC-82-11 - Register Both Halves of a Key Pair

411 Register a private key and a public key and set the Link attribute to point to each other. Verify
412 the links were set correctly by locating the keys based on the link attributes, and then delete
413 both objects.

# TIME 0	
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>

0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="PrivateKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Sign"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-82-11-prikey"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<PrivateKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="PKCS_8"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString" value="30820276020100300d06092a864886f70d0101010500048202603082025c02010002818100930451c9ecd94f5bb9da17dd09381bd23be43eca8c7539f301fc8a8cd5d5274c3e7699dbdc711c97a7aa91e2c50a82bd0b1034f0df493dec16362427e58acce7f6ce0f9bcc617bbd8c90d0094a2703ba0d09eb19d1005f2fb265526aac75af32f8bc782cded2a57f811e03eaf67a944de5e78413dca8f232d074e6dcea4cec9f02030100010281800b6a7d736199ea48a420e4537ca0c7c046784dcbeaa63baebc0bc132787449cde8d7cad0c0c863c0fefb06c3062befc50033ecf87b4e33a9be7bcbcb8f1511ae215e80deb5d8af2bd31319d7821196640935a0cd67c94599579f2100d65e038831fdafb0dbe2bbdac00a696e67e756350e1c99ace11a36dabac3ed3e730960059024100ddf672fbcc5bda3d73affc4e791e0c03390224405d69ccaabc749faa0dcd4c2583c71dde8941a7b9aa030f52ef1451466c074d4d338fe677892acd9e10fd35bd024100a98fbc3ed6b4c6f860f97165ac2f7bb6f2e2cb192a9abd49795be5bcf37d8ee69a6e169c24e5c32e4e7fa33265461407f952ba49e204818a2f785f113f922b8b0240253f9470390d39049303777ddbcb9750e9d64849ce0903eae704dc9f589b7680deb9d609fd5bcd4decdd6f120542e5cff5d76f2a43c8615fb5b3a9213463797aa9024100alddf023c0cd94c019bb26d09b9e3ca8fa971cb16aa58b9baf79d6081aldbba452ba53653e2804ba98ff69e8bb1b3a161ea225ea501463216a8dab9b88a75e5f02406178646e112cf79d921a8a843f17f6e7ff974f688122365bf6690cdfc996e1890952eb3820dd1890ec1c8619e87a2bd38f9d03b37fac742efb748c7885942c39"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0030	<CryptographicLength type="Integer" value="1024"/>
0031	</KeyBlock>
0032	</PrivateKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="1"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>

0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="1"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PublicKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0068	<AttributeValue type="Integer" value="Verify"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>
0073	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0075	</AttributeValue>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-82-11-
	pubkey"/>
0080	</Attribute>
0081	</TemplateAttribute>
0082	<PublicKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="X_509"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString"
	value="30819f300d06092a864886f70d010101050003818d0030818902818100930
	451c9ecd94f5bb9da17dd09381bd23be43eca8c7539f301fc8a8cd5d5274c3e7699d
	bdc711c97a7aa91e2c50a82bd0b1034f0df493dec16362427e58acce7f6ce0f9bcc6
	17bbd8c90d0094a2703ba0d09eb19d1005f2fb265526aac75af32f8bc782cded2a57
	f811e03eaf67a944de5e78413dca8f232d074e6dcea4cec9f0203010001"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0089	<CryptographicLength type="Integer" value="1024"/>
0090	</KeyBlock>
0091	</PublicKey>
0092	</RequestPayload>

0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="1"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0109	</ResponsePayload>
0110	</BatchItem>
0111	</ResponseMessage>
	# TIME 2
0112	<RequestMessage>
0113	<RequestHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="1"/>
0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="AddAttribute"/>
0122	<RequestPayload>
0123	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Link"/>
0126	<AttributeValue>
0127	<LinkType type="Enumeration" value="PublicKeyLink"/>
0128	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0129	</AttributeValue>
0130	</Attribute>
0131	</RequestPayload>
0132	</BatchItem>
0133	</RequestMessage>
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="1"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="AddAttribute"/>

0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0148	<Attribute>
0149	<AttributeName type="TextString" value="Link"/>
0150	<AttributeValue>
0151	<LinkType type="Enumeration" value="PublicKeyLink"/>
0152	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0153	</AttributeValue>
0154	</Attribute>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
# TIME 3	
0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="1"/>
0163	</ProtocolVersion>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Locate"/>
0168	<RequestPayload>
0169	<Attribute>
0170	<AttributeName type="TextString" value="Object Type"/>
0171	<AttributeValue type="Enumeration" value="PublicKey"/>
0172	</Attribute>
0173	<Attribute>
0174	<AttributeName type="TextString" value="Link"/>
0175	<AttributeValue>
0176	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0177	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0178	</AttributeValue>
0179	</Attribute>
0180	</RequestPayload>
0181	</BatchItem>
0182	</RequestMessage>
0183	<ResponseMessage>
0184	<ResponseHeader>
0185	<ProtocolVersion>
0186	<ProtocolVersionMajor type="Integer" value="1"/>
0187	<ProtocolVersionMinor type="Integer" value="1"/>
0188	</ProtocolVersion>
0189	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0190	<BatchCount type="Integer" value="1"/>
0191	</ResponseHeader>
0192	<BatchItem>
0193	<Operation type="Enumeration" value="Locate"/>
0194	<ResultStatus type="Enumeration" value="Success"/>
0195	<ResponsePayload>
0196	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>

0197	</ResponsePayload>
0198	</BatchItem>
0199	</ResponseMessage>
0200	# TIME 4
0200	<RequestMessage>
0201	<RequestHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="1"/>
0205	</ProtocolVersion>
0206	<BatchCount type="Integer" value="1"/>
0207	</RequestHeader>
0208	<BatchItem>
0209	<Operation type="Enumeration" value="Locate"/>
0210	<RequestPayload>
0211	<Attribute>
0212	<AttributeName type="TextString" value="Object Type"/>
0213	<AttributeValue type="Enumeration" value="PrivateKey"/>
0214	</Attribute>
0215	<Attribute>
0216	<AttributeName type="TextString" value="Link"/>
0217	<AttributeValue>
0218	<LinkType type="Enumeration" value="PublicKeyLink"/>
0219	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0220	</AttributeValue>
0221	</Attribute>
0222	</RequestPayload>
0223	</BatchItem>
0224	</RequestMessage>
0225	<ResponseMessage>
0226	<ResponseHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="1"/>
0230	</ProtocolVersion>
0231	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0232	<BatchCount type="Integer" value="1"/>
0233	</ResponseHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="Locate"/>
0236	<ResultStatus type="Enumeration" value="Success"/>
0237	<ResponsePayload>
0238	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0239	</ResponsePayload>
0240	</BatchItem>
0241	</ResponseMessage>
0242	# TIME 5
0242	<RequestMessage>
0243	<RequestHeader>
0244	<ProtocolVersion>
0245	<ProtocolVersionMajor type="Integer" value="1"/>
0246	<ProtocolVersionMinor type="Integer" value="1"/>
0247	</ProtocolVersion>
0248	<BatchCount type="Integer" value="1"/>

0249	</RequestHeader>
0250	<BatchItem>
0251	<Operation type="Enumeration" value="Destroy"/>
0252	<RequestPayload>
0253	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0254	</RequestPayload>
0255	</BatchItem>
0256	</RequestMessage>
0257	<ResponseMessage>
0258	<ResponseHeader>
0259	<ProtocolVersion>
0260	<ProtocolVersionMajor type="Integer" value="1"/>
0261	<ProtocolVersionMinor type="Integer" value="1"/>
0262	</ProtocolVersion>
0263	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0264	<BatchCount type="Integer" value="1"/>
0265	</ResponseHeader>
0266	<BatchItem>
0267	<Operation type="Enumeration" value="Destroy"/>
0268	<ResultStatus type="Enumeration" value="Success"/>
0269	<ResponsePayload>
0270	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0271	</ResponsePayload>
0272	</BatchItem>
0273	</ResponseMessage>
	# TIME 6
0274	<RequestMessage>
0275	<RequestHeader>
0276	<ProtocolVersion>
0277	<ProtocolVersionMajor type="Integer" value="1"/>
0278	<ProtocolVersionMinor type="Integer" value="1"/>
0279	</ProtocolVersion>
0280	<BatchCount type="Integer" value="1"/>
0281	</RequestHeader>
0282	<BatchItem>
0283	<Operation type="Enumeration" value="Destroy"/>
0284	<RequestPayload>
0285	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0286	</RequestPayload>
0287	</BatchItem>
0288	</RequestMessage>
0289	<ResponseMessage>
0290	<ResponseHeader>
0291	<ProtocolVersion>
0292	<ProtocolVersionMajor type="Integer" value="1"/>
0293	<ProtocolVersionMinor type="Integer" value="1"/>
0294	</ProtocolVersion>
0295	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0296	<BatchCount type="Integer" value="1"/>
0297	</ResponseHeader>
0298	<BatchItem>
0299	<Operation type="Enumeration" value="Destroy"/>
0300	<ResultStatus type="Enumeration" value="Success"/>

0301	<ResponsePayload>
0302	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0303	</ResponsePayload>
0304	</BatchItem>
0305	</ResponseMessage>

414

415 2.2.14 TC-91-11 - Create a Key, Re-key

416 Create a symmetric key with a specific name, and then use Locate to find the key. After using
417 Re-key to create a new key, verify that the name was removed from the existing key and copied
418 to the new key. Also verify that the key material for the old key is still retrievable. To clean up,
419 both keys are deleted.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="TC-91-11-rekeyKey"/>
0030	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0031	</AttributeValue>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	</BatchItem>

0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="1"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
# TIME 1	
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="1"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="Locate"/>
0065	<RequestPayload>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Name"/>
0068	<AttributeValue>
0069	<NameValue type="TextString" value="TC-91-11-rekeyKey"/>
0070	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0071	</AttributeValue>
0072	</Attribute>
0073	</RequestPayload>
0074	</BatchItem>
0075	</RequestMessage>
0076	<ResponseMessage>
0077	<ResponseHeader>
0078	<ProtocolVersion>
0079	<ProtocolVersionMajor type="Integer" value="1"/>
0080	<ProtocolVersionMinor type="Integer" value="1"/>
0081	</ProtocolVersion>
0082	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0083	<BatchCount type="Integer" value="1"/>
0084	</ResponseHeader>
0085	<BatchItem>
0086	<Operation type="Enumeration" value="Locate"/>
0087	<ResultStatus type="Enumeration" value="Success"/>
0088	<ResponsePayload>

0089	<UniqueIdentifier type="TextString"
0090	value="\$UNIQUE_IDENTIFIER_0"/>
0091	</ResponsePayload>
0092	</BatchItem>
0092	</ResponseMessage>
# TIME 2	
0093	<RequestMessage>
0094	<RequestHeader>
0095	<ProtocolVersion>
0096	<ProtocolVersionMajor type="Integer" value="1"/>
0097	<ProtocolVersionMinor type="Integer" value="1"/>
0098	</ProtocolVersion>
0099	<BatchCount type="Integer" value="1"/>
0100	</RequestHeader>
0101	<BatchItem>
0102	<Operation type="Enumeration" value="ReKey"/>
0103	<RequestPayload>
0104	<UniqueIdentifier type="TextString"
0105	value="\$UNIQUE_IDENTIFIER_0"/>
0106	</RequestPayload>
0107	</BatchItem>
0107	</RequestMessage>
0108	<ResponseMessage>
0109	<ResponseHeader>
0110	<ProtocolVersion>
0111	<ProtocolVersionMajor type="Integer" value="1"/>
0112	<ProtocolVersionMinor type="Integer" value="1"/>
0113	</ProtocolVersion>
0114	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0115	<BatchCount type="Integer" value="1"/>
0116	</ResponseHeader>
0117	<BatchItem>
0118	<Operation type="Enumeration" value="ReKey"/>
0119	<ResultStatus type="Enumeration" value="Success"/>
0120	<ResponsePayload>
0121	<UniqueIdentifier type="TextString"
0122	value="\$UNIQUE_IDENTIFIER_1"/>
0123	</ResponsePayload>
0124	</BatchItem>
0124	</ResponseMessage>
# TIME 3	
0125	<RequestMessage>
0126	<RequestHeader>
0127	<ProtocolVersion>
0128	<ProtocolVersionMajor type="Integer" value="1"/>
0129	<ProtocolVersionMinor type="Integer" value="1"/>
0130	</ProtocolVersion>
0131	<BatchCount type="Integer" value="1"/>
0132	</RequestHeader>
0133	<BatchItem>
0134	<Operation type="Enumeration" value="Locate"/>
0135	<RequestPayload>
0136	<Attribute>
0137	<AttributeName type="TextString" value="Name"/>
0138	<AttributeValue>
0139	<NameValue type="TextString" value="TC-91-11-rekeyKey"/>

0140	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0141	</AttributeValue>
0142	</Attribute>
0143	</RequestPayload>
0144	</BatchItem>
0145	</RequestMessage>
0146	<ResponseMessage>
0147	<ResponseHeader>
0148	<ProtocolVersion>
0149	<ProtocolVersionMajor type="Integer" value="1"/>
0150	<ProtocolVersionMinor type="Integer" value="1"/>
0151	</ProtocolVersion>
0152	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0153	<BatchCount type="Integer" value="1"/>
0154	</ResponseHeader>
0155	<BatchItem>
0156	<Operation type="Enumeration" value="Locate"/>
0157	<ResultStatus type="Enumeration" value="Success"/>
0158	<ResponsePayload>
0159	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0160	</ResponsePayload>
0161	</BatchItem>
0162	</ResponseMessage>
	# TIME 4
0163	<RequestMessage>
0164	<RequestHeader>
0165	<ProtocolVersion>
0166	<ProtocolVersionMajor type="Integer" value="1"/>
0167	<ProtocolVersionMinor type="Integer" value="1"/>
0168	</ProtocolVersion>
0169	<BatchCount type="Integer" value="1"/>
0170	</RequestHeader>
0171	<BatchItem>
0172	<Operation type="Enumeration" value="GetAttributes"/>
0173	<RequestPayload>
0174	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0175	<AttributeName type="TextString" value="Name"/>
0176	</RequestPayload>
0177	</BatchItem>
0178	</RequestMessage>
0179	<ResponseMessage>
0180	<ResponseHeader>
0181	<ProtocolVersion>
0182	<ProtocolVersionMajor type="Integer" value="1"/>
0183	<ProtocolVersionMinor type="Integer" value="1"/>
0184	</ProtocolVersion>
0185	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0186	<BatchCount type="Integer" value="1"/>
0187	</ResponseHeader>
0188	<BatchItem>
0189	<Operation type="Enumeration" value="GetAttributes"/>
0190	<ResultStatus type="Enumeration" value="Success"/>
0191	<ResponsePayload>

0192	<UniqueIdentifier type="TextString"
0193	value="\$UNIQUE_IDENTIFIER_0"/>
0194	</ResponsePayload>
0195	</BatchItem>
0196	</ResponseMessage>
# TIME 5	
0196	<RequestMessage>
0197	<RequestHeader>
0198	<ProtocolVersion>
0199	<ProtocolVersionMajor type="Integer" value="1"/>
0200	<ProtocolVersionMinor type="Integer" value="1"/>
0201	</ProtocolVersion>
0202	<BatchCount type="Integer" value="1"/>
0203	</RequestHeader>
0204	<BatchItem>
0205	<Operation type="Enumeration" value="Get"/>
0206	<RequestPayload>
0207	<UniqueIdentifier type="TextString"
0208	value="\$UNIQUE_IDENTIFIER_0"/>
0209	</RequestPayload>
0210	</BatchItem>
0211	</RequestMessage>
0212	<ResponseMessage>
0213	<ResponseHeader>
0214	<ProtocolVersion>
0215	<ProtocolVersionMajor type="Integer" value="1"/>
0216	<ProtocolVersionMinor type="Integer" value="1"/>
0217	</ProtocolVersion>
0218	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0219	<BatchCount type="Integer" value="1"/>
0220	</ResponseHeader>
0221	<BatchItem>
0222	<Operation type="Enumeration" value="Get"/>
0223	<ResultStatus type="Enumeration" value="Success"/>
0224	<ResponsePayload>
0225	<ObjectType type="Enumeration" value="SymmetricKey"/>
0226	<UniqueIdentifier type="TextString"
0227	value="\$UNIQUE_IDENTIFIER_0"/>
0228	<SymmetricKey>
0229	<KeyBlock>
0230	<KeyFormatType type="Enumeration" value="Raw"/>
0231	<KeyMaterial type="ByteString"
0232	value="9ca9840291a65889043c37707da997e8"/>
0233	</KeyMaterial>
0234	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0235	<CryptographicLength type="Integer" value="128"/>
0236	</CryptographicLength>
0237	</KeyBlock>
0238	</SymmetricKey>
0239	</ResponsePayload>
0240	</BatchItem>
0241	</ResponseMessage>
# TIME 6	
0239	<RequestMessage>
0240	<RequestHeader>
0241	<ProtocolVersion>

0242	<ProtocolVersionMajor type="Integer" value="1"/>
0243	<ProtocolVersionMinor type="Integer" value="1"/>
0244	</ProtocolVersion>
0245	<BatchCount type="Integer" value="1"/>
0246	</RequestHeader>
0247	<BatchItem>
0248	<Operation type="Enumeration" value="Destroy"/>
0249	<RequestPayload>
0250	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0251	</RequestPayload>
0252	</BatchItem>
0253	</RequestMessage>
0254	<ResponseMessage>
0255	<ResponseHeader>
0256	<ProtocolVersion>
0257	<ProtocolVersionMajor type="Integer" value="1"/>
0258	<ProtocolVersionMinor type="Integer" value="1"/>
0259	</ProtocolVersion>
0260	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0261	<BatchCount type="Integer" value="1"/>
0262	</ResponseHeader>
0263	<BatchItem>
0264	<Operation type="Enumeration" value="Destroy"/>
0265	<ResultStatus type="Enumeration" value="Success"/>
0266	<ResponsePayload>
0267	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0268	</ResponsePayload>
0269	</BatchItem>
0270	</ResponseMessage>
	# TIME 7
0271	<RequestMessage>
0272	<RequestHeader>
0273	<ProtocolVersion>
0274	<ProtocolVersionMajor type="Integer" value="1"/>
0275	<ProtocolVersionMinor type="Integer" value="1"/>
0276	</ProtocolVersion>
0277	<BatchCount type="Integer" value="1"/>
0278	</RequestHeader>
0279	<BatchItem>
0280	<Operation type="Enumeration" value="Destroy"/>
0281	<RequestPayload>
0282	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0283	</RequestPayload>
0284	</BatchItem>
0285	</RequestMessage>
0286	<ResponseMessage>
0287	<ResponseHeader>
0288	<ProtocolVersion>
0289	<ProtocolVersionMajor type="Integer" value="1"/>
0290	<ProtocolVersionMinor type="Integer" value="1"/>
0291	</ProtocolVersion>
0292	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0293	<BatchCount type="Integer" value="1"/>

0294	</ResponseHeader>
0295	<BatchItem>
0296	<Operation type="Enumeration" value="Destroy"/>
0297	<ResultStatus type="Enumeration" value="Success"/>
0298	<ResponsePayload>
0299	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0300	</ResponsePayload>
0301	</BatchItem>
0302	</ResponseMessage>

420

421 2.2.15 TC-92-11 - Existing Key Expired, Re-key with Same Life-cycle

422 Create a new symmetric key. Then add the Activation Date and Deactivation Date attributes
423 based on the timestamp in the response to the Create request. The Activation Date is set to the
424 current time and the Deactivation Date to a time in the near future. Repeated Get Attribute calls
425 are performed to verify that the state is first 'Active', then subsequently 'Deactivated'. Then
426 issue a Re-key request, including an Offset value of zero leading to the Activation Date of the
427 replacement key to be set to the same value as the Initial Date of the replacement key. Verify
428 from the response that the Activation Date and Deactivation Date attributes were set correctly
429 (if they are not returned, issue a Get Attribute request). Do a Get Attribute operation to verify
430 that the state of the new key is 'Active'. To clean up, both keys are deleted.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	</Attribute>

0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="TC-92-11-rekeyKey"/>
0030	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0031	</AttributeValue>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="1"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2012-04-27T08:12:27+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
	# TIME 1
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="1"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="2"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="AddAttribute"/>
0065	<UniqueBatchItemID type="ByteString" value="606051f958d79b0f"/>
0066	<RequestPayload>
0067	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0068	<Attribute>
0069	<AttributeName type="TextString" value="Activation Date"/>
0070	<AttributeValue type="DateTime" value="\$NOW"/>
0071	</Attribute>
0072	</RequestPayload>
0073	</BatchItem>
0074	<BatchItem>
0075	<Operation type="Enumeration" value="AddAttribute"/>
0076	<UniqueBatchItemID type="ByteString" value="7cb12802f6a52cf1"/>
0077	<RequestPayload>
0078	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0079	<Attribute>
0080	<AttributeName type="TextString" value="Deactivation Date"/>
0081	<AttributeValue type="DateTime" value="\$NOW+120"/>
0082	</Attribute>
0083	</RequestPayload>
0084	</BatchItem>
0085	</RequestMessage>
0086	<ResponseMessage>
0087	<ResponseHeader>
0088	<ProtocolVersion>
0089	<ProtocolVersionMajor type="Integer" value="1"/>
0090	<ProtocolVersionMinor type="Integer" value="1"/>
0091	</ProtocolVersion>
0092	<TimeStamp type="DateTime" value="2012-04-27T08:12:27+00:00"/>
0093	<BatchCount type="Integer" value="2"/>
0094	</ResponseHeader>
0095	<BatchItem>
0096	<Operation type="Enumeration" value="AddAttribute"/>
0097	<UniqueBatchItemID type="ByteString" value="606051f958d79b0f"/>
0098	<ResultStatus type="Enumeration" value="Success"/>
0099	<ResponsePayload>
0100	<UniqueIdentifier type="TextString"
0101	value="\$UNIQUE_IDENTIFIER_0"/>
0101	<Attribute>
0102	<AttributeName type="TextString" value="Activation Date"/>
0103	<AttributeValue type="DateTime" value="\$NOW"/>
0104	</Attribute>
0105	</ResponsePayload>
0106	</BatchItem>
0107	<BatchItem>
0108	<Operation type="Enumeration" value="AddAttribute"/>
0109	<UniqueBatchItemID type="ByteString" value="7cb12802f6a52cf1"/>
0110	<ResultStatus type="Enumeration" value="Success"/>
0111	<ResponsePayload>
0112	<UniqueIdentifier type="TextString"
0113	value="\$UNIQUE_IDENTIFIER_0"/>
0113	<Attribute>
0114	<AttributeName type="TextString" value="Deactivation Date"/>
0115	<AttributeValue type="DateTime" value="\$NOW+120"/>
0116	</Attribute>
0117	</ResponsePayload>
0118	</BatchItem>
0119	</ResponseMessage>
	# TIME 2
	# [REPEAT] until GetAttributes response shows State changed to Deactivated
0120	<RequestMessage>
0121	<RequestHeader>
0122	<ProtocolVersion>
0123	<ProtocolVersionMajor type="Integer" value="1"/>
0124	<ProtocolVersionMinor type="Integer" value="1"/>
0125	</ProtocolVersion>
0126	<BatchCount type="Integer" value="1"/>
0127	</RequestHeader>
0128	<BatchItem>
0129	<Operation type="Enumeration" value="GetAttributes"/>
0130	<RequestPayload>

0131	<UniqueIdentifier type="TextString"
0132	value="\$UNIQUE_IDENTIFIER_0"/>
0133	<AttributeName type="TextString" value="State"/>
0134	</RequestPayload>
0135	</BatchItem>
0136	</RequestMessage>
0137	<ResponseMessage>
0138	<ResponseHeader>
0139	<ProtocolVersion>
0140	<ProtocolVersionMajor type="Integer" value="1"/>
0141	<ProtocolVersionMinor type="Integer" value="1"/>
0142	</ProtocolVersion>
0143	<TimeStamp type="DateTime" value="2012-04-27T08:12:27+00:00"/>
0144	<BatchCount type="Integer" value="1"/>
0145	</ResponseHeader>
0146	<BatchItem>
0147	<Operation type="Enumeration" value="GetAttributes"/>
0148	<ResultStatus type="Enumeration" value="Success"/>
0149	<ResponsePayload>
0150	<UniqueIdentifier type="TextString"
0151	value="\$UNIQUE_IDENTIFIER_0"/>
0152	<Attribute>
0153	<AttributeName type="TextString" value="State"/>
0154	<AttributeValue type="Enumeration" value="Active"/>
0155	</Attribute>
0156	</ResponsePayload>
0157	</BatchItem>
0158	</ResponseMessage>
0159	# TIME 3
0160	<RequestMessage>
0161	<RequestHeader>
0162	<ProtocolVersion>
0163	<ProtocolVersionMajor type="Integer" value="1"/>
0164	<ProtocolVersionMinor type="Integer" value="1"/>
0165	</ProtocolVersion>
0166	<BatchCount type="Integer" value="1"/>
0167	</RequestHeader>
0168	<BatchItem>
0169	<Operation type="Enumeration" value="GetAttributes"/>
0170	<RequestPayload>
0171	<UniqueIdentifier type="TextString"
0172	value="\$UNIQUE_IDENTIFIER_0"/>
0173	<AttributeName type="TextString" value="State"/>
0174	</RequestPayload>
0175	</BatchItem>
0176	</RequestMessage>
0177	<ResponseMessage>
0178	<ResponseHeader>
0179	<ProtocolVersion>
0180	<ProtocolVersionMajor type="Integer" value="1"/>
0181	<ProtocolVersionMinor type="Integer" value="1"/>
0182	</ProtocolVersion>
	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
	<BatchCount type="Integer" value="1"/>
	</ResponseHeader>
	<BatchItem>

0183	<Operation type="Enumeration" value="GetAttributes"/>
0184	<ResultStatus type="Enumeration" value="Success"/>
0185	<ResponsePayload>
0186	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0187	<Attribute>
0188	<AttributeName type="TextString" value="State"/>
0189	<AttributeValue type="Enumeration" value="Deactivated"/>
0190	</Attribute>
0191	</ResponsePayload>
0192	</BatchItem>
0193	</ResponseMessage>
	# TIME 4
0194	<RequestMessage>
0195	<RequestHeader>
0196	<ProtocolVersion>
0197	<ProtocolVersionMajor type="Integer" value="1"/>
0198	<ProtocolVersionMinor type="Integer" value="1"/>
0199	</ProtocolVersion>
0200	<BatchCount type="Integer" value="1"/>
0201	</RequestHeader>
0202	<BatchItem>
0203	<Operation type="Enumeration" value="ReKey"/>
0204	<RequestPayload>
0205	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0206	<Offset type="Interval" value="0"/>
0207	</RequestPayload>
0208	</BatchItem>
0209	</RequestMessage>
0210	<ResponseMessage>
0211	<ResponseHeader>
0212	<ProtocolVersion>
0213	<ProtocolVersionMajor type="Integer" value="1"/>
0214	<ProtocolVersionMinor type="Integer" value="1"/>
0215	</ProtocolVersion>
0216	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0217	<BatchCount type="Integer" value="1"/>
0218	</ResponseHeader>
0219	<BatchItem>
0220	<Operation type="Enumeration" value="ReKey"/>
0221	<ResultStatus type="Enumeration" value="Success"/>
0222	<ResponsePayload>
0223	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0224	</ResponsePayload>
0225	</BatchItem>
0226	</ResponseMessage>
	# TIME 5
0227	<RequestMessage>
0228	<RequestHeader>
0229	<ProtocolVersion>
0230	<ProtocolVersionMajor type="Integer" value="1"/>
0231	<ProtocolVersionMinor type="Integer" value="1"/>
0232	</ProtocolVersion>
0233	<BatchCount type="Integer" value="1"/>

0234	</RequestHeader>
0235	<BatchItem>
0236	<Operation type="Enumeration" value="GetAttributes"/>
0237	<RequestPayload>
0238	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0239	<AttributeName type="TextString" value="Activation Date"/>
0240	<AttributeName type="TextString" value="Deactivation Date"/>
0241	</RequestPayload>
0242	</BatchItem>
0243	</RequestMessage>
0244	<ResponseMessage>
0245	<ResponseHeader>
0246	<ProtocolVersion>
0247	<ProtocolVersionMajor type="Integer" value="1"/>
0248	<ProtocolVersionMinor type="Integer" value="1"/>
0249	</ProtocolVersion>
0250	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0251	<BatchCount type="Integer" value="1"/>
0252	</ResponseHeader>
0253	<BatchItem>
0254	<Operation type="Enumeration" value="GetAttributes"/>
0255	<ResultStatus type="Enumeration" value="Success"/>
0256	<ResponsePayload>
0257	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0258	<Attribute>
0259	<AttributeName type="TextString" value="Activation Date"/>
0260	<AttributeValue type="DateTime" value="\$NOW"/>
0261	</Attribute>
0262	<Attribute>
0263	<AttributeName type="TextString" value="Deactivation Date"/>
0264	<AttributeValue type="DateTime" value="\$NOW+120"/>
0265	</Attribute>
0266	</ResponsePayload>
0267	</BatchItem>
0268	</ResponseMessage>
	# TIME 6
0269	<RequestMessage>
0270	<RequestHeader>
0271	<ProtocolVersion>
0272	<ProtocolVersionMajor type="Integer" value="1"/>
0273	<ProtocolVersionMinor type="Integer" value="1"/>
0274	</ProtocolVersion>
0275	<BatchCount type="Integer" value="1"/>
0276	</RequestHeader>
0277	<BatchItem>
0278	<Operation type="Enumeration" value="GetAttributes"/>
0279	<RequestPayload>
0280	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0281	<AttributeName type="TextString" value="State"/>
0282	</RequestPayload>
0283	</BatchItem>
0284	</RequestMessage>
0285	<ResponseMessage>

0286	<ResponseHeader>
0287	<ProtocolVersion>
0288	<ProtocolVersionMajor type="Integer" value="1"/>
0289	<ProtocolVersionMinor type="Integer" value="1"/>
0290	</ProtocolVersion>
0291	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0292	<BatchCount type="Integer" value="1"/>
0293	</ResponseHeader>
0294	<BatchItem>
0295	<Operation type="Enumeration" value="GetAttributes"/>
0296	<ResultStatus type="Enumeration" value="Success"/>
0297	<ResponsePayload>
0298	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0299	<Attribute>
0300	<AttributeName type="TextString" value="State"/>
0301	<AttributeValue type="Enumeration" value="Active"/>
0302	</Attribute>
0303	</ResponsePayload>
0304	</BatchItem>
0305	</ResponseMessage>
# TIME 7	
0306	<RequestMessage>
0307	<RequestHeader>
0308	<ProtocolVersion>
0309	<ProtocolVersionMajor type="Integer" value="1"/>
0310	<ProtocolVersionMinor type="Integer" value="1"/>
0311	</ProtocolVersion>
0312	<BatchCount type="Integer" value="1"/>
0313	</RequestHeader>
0314	<BatchItem>
0315	<Operation type="Enumeration" value="Destroy"/>
0316	<RequestPayload>
0317	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0318	</RequestPayload>
0319	</BatchItem>
0320	</RequestMessage>
0321	<ResponseMessage>
0322	<ResponseHeader>
0323	<ProtocolVersion>
0324	<ProtocolVersionMajor type="Integer" value="1"/>
0325	<ProtocolVersionMinor type="Integer" value="1"/>
0326	</ProtocolVersion>
0327	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0328	<BatchCount type="Integer" value="1"/>
0329	</ResponseHeader>
0330	<BatchItem>
0331	<Operation type="Enumeration" value="Destroy"/>
0332	<ResultStatus type="Enumeration" value="Success"/>
0333	<ResponsePayload>
0334	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0335	</ResponsePayload>
0336	</BatchItem>
0337	</ResponseMessage>

0338 0339 0340 0341 0342 0343 0344 0345 0346 0347 0348 0349 0350 0351 0352 0353 0354 0355 0356 0357 0358 0359 0360 0361 0362 0363 0364	# TIME 8 <RequestMessage> <RequestHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="1"/> </ProtocolVersion> <BatchOrderOption type="Boolean" value="true"/> <BatchCount type="Integer" value="2"/> </RequestHeader> <BatchItem> <Operation type="Enumeration" value="Revoke"/> <UniqueBatchItemID type="ByteString" value="955dfbb9abbec308"/> <RequestPayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> <RevocationReason> <RevocationReasonCode type="Enumeration" value="CessationOfOperation"/> </RevocationReason> </RequestPayload> </BatchItem> <BatchItem> <Operation type="Enumeration" value="Destroy"/> <UniqueBatchItemID type="ByteString" value="6ce5ea0c8334b076"/> <RequestPayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> </RequestPayload> </BatchItem> </RequestMessage>
0365 0366 0367 0368 0369 0370 0371 0372 0373 0374 0375 0376 0377 0378 0379 0380 0381 0382 0383 0384 0385 0386 0387 0388	<ResponseMessage> <ResponseHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="1"/> </ProtocolVersion> <TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/> <BatchCount type="Integer" value="2"/> </ResponseHeader> <BatchItem> <Operation type="Enumeration" value="Revoke"/> <UniqueBatchItemID type="ByteString" value="955dfbb9abbec308"/> <ResultStatus type="Enumeration" value="Success"/> <ResponsePayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> </ResponsePayload> </BatchItem> <BatchItem> <Operation type="Enumeration" value="Destroy"/> <UniqueBatchItemID type="ByteString" value="6ce5ea0c8334b076"/> <ResultStatus type="Enumeration" value="Success"/> <ResponsePayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> </ResponsePayload>

0389	</BatchItem>
0390	</ResponseMessage>

431

432 2.2.16 TC-93-11 - Existing Key Compromised, Re-key with Same Life-cycle

433 Create a new symmetric key with the Activation Date in the past. Do a Get Attribute operation
434 on the State attribute to verify the key is 'Active'. Then revoke the key as compromised, verify
435 that the state has changed to 'Compromised'. Create a replacement key using Re-key with the
436 offset set to '0' to indicate that the times are to be copied from the existing key. Do a Get
437 Attribute operation to verify that the state of the new key is 'Active'. To clean up, both keys are
438 deleted.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Length"/>
0022	<AttributeValue type="Integer" value="128"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Cryptographic
0026	Usage Mask"/>
0027	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="Activation Date"/>
0031	<AttributeValue type="DateTime" value="\$NOW"/>
0032	</Attribute>
0033	<Attribute>
0034	<AttributeName type="TextString" value="Name"/>
0035	<AttributeValue type="TextString" value="TC-93-11-rekeyKey"/>
0036	<NameType type="Enumeration"
0037	value="UninterpretedTextString"/>
	</Attribute>
	</TemplateAttribute>

0038	</RequestPayload>
0039	</BatchItem>
0040	</RequestMessage>
0041	<ResponseMessage>
0042	<ResponseHeader>
0043	<ProtocolVersion>
0044	<ProtocolVersionMajor type="Integer" value="1"/>
0045	<ProtocolVersionMinor type="Integer" value="1"/>
0046	</ProtocolVersion>
0047	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0048	<BatchCount type="Integer" value="1"/>
0049	</ResponseHeader>
0050	<BatchItem>
0051	<Operation type="Enumeration" value="Create"/>
0052	<ResultStatus type="Enumeration" value="Success"/>
0053	<ResponsePayload>
0054	<ObjectType type="Enumeration" value="SymmetricKey"/>
0055	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0056	</ResponsePayload>
0057	</BatchItem>
0058	</ResponseMessage>
	# TIME 1
0059	<RequestMessage>
0060	<RequestHeader>
0061	<ProtocolVersion>
0062	<ProtocolVersionMajor type="Integer" value="1"/>
0063	<ProtocolVersionMinor type="Integer" value="1"/>
0064	</ProtocolVersion>
0065	<BatchCount type="Integer" value="1"/>
0066	</RequestHeader>
0067	<BatchItem>
0068	<Operation type="Enumeration" value="GetAttributes"/>
0069	<RequestPayload>
0070	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0071	<AttributeName type="TextString" value="State"/>
0072	</RequestPayload>
0073	</BatchItem>
0074	</RequestMessage>
0075	<ResponseMessage>
0076	<ResponseHeader>
0077	<ProtocolVersion>
0078	<ProtocolVersionMajor type="Integer" value="1"/>
0079	<ProtocolVersionMinor type="Integer" value="1"/>
0080	</ProtocolVersion>
0081	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0082	<BatchCount type="Integer" value="1"/>
0083	</ResponseHeader>
0084	<BatchItem>
0085	<Operation type="Enumeration" value="GetAttributes"/>
0086	<ResultStatus type="Enumeration" value="Success"/>
0087	<ResponsePayload>
0088	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0089	<Attribute>

0090	<AttributeName type="TextString" value="State"/>
0091	<AttributeValue type="Enumeration" value="Active"/>
0092	</Attribute>
0093	</ResponsePayload>
0094	</BatchItem>
0095	</ResponseMessage>
# TIME 2	
0096	<RequestMessage>
0097	<RequestHeader>
0098	<ProtocolVersion>
0099	<ProtocolVersionMajor type="Integer" value="1"/>
0100	<ProtocolVersionMinor type="Integer" value="1"/>
0101	</ProtocolVersion>
0102	<BatchCount type="Integer" value="1"/>
0103	</RequestHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Revoke"/>
0106	<RequestPayload>
0107	<UniqueIdentifier type="TextString"
0108	value="\$UNIQUE_IDENTIFIER_0"/>
0109	<RevocationReason>
0110	<RevocationReasonCode type="Enumeration"
0111	value="KeyCompromise"/>
0112	</RevocationReason>
0113	<CompromiseOccurrenceDate type="DateTime" value="\$NOW"/>
0114	</RequestPayload>
0115	</BatchItem>
0116	</RequestMessage>
0117	<ResponseMessage>
0118	<ResponseHeader>
0119	<ProtocolVersion>
0120	<ProtocolVersionMajor type="Integer" value="1"/>
0121	<ProtocolVersionMinor type="Integer" value="1"/>
0122	</ProtocolVersion>
0123	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0124	<BatchCount type="Integer" value="1"/>
0125	</ResponseHeader>
0126	<BatchItem>
0127	<Operation type="Enumeration" value="Revoke"/>
0128	<ResultStatus type="Enumeration" value="Success"/>
0129	<ResponsePayload>
0130	<UniqueIdentifier type="TextString"
0131	value="\$UNIQUE_IDENTIFIER_0"/>
0132	</ResponsePayload>
0133	</BatchItem>
0134	</ResponseMessage>
# TIME 3	
0135	<RequestMessage>
0136	<RequestHeader>
0137	<ProtocolVersion>
0138	<ProtocolVersionMajor type="Integer" value="1"/>
0139	<ProtocolVersionMinor type="Integer" value="1"/>
0140	</ProtocolVersion>
	<BatchCount type="Integer" value="1"/>
	</RequestHeader>
	<BatchItem>

0141	<Operation type="Enumeration" value="GetAttributes"/>
0142	<RequestPayload>
0143	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0144	<AttributeName type="TextString" value="State"/>
0145	</RequestPayload>
0146	</BatchItem>
0147	</RequestMessage>
0148	<ResponseMessage>
0149	<ResponseHeader>
0150	<ProtocolVersion>
0151	<ProtocolVersionMajor type="Integer" value="1"/>
0152	<ProtocolVersionMinor type="Integer" value="1"/>
0153	</ProtocolVersion>
0154	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0155	<BatchCount type="Integer" value="1"/>
0156	</ResponseHeader>
0157	<BatchItem>
0158	<Operation type="Enumeration" value="GetAttributes"/>
0159	<ResultStatus type="Enumeration" value="Success"/>
0160	<ResponsePayload>
0161	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0162	<Attribute>
0163	<AttributeName type="TextString" value="State"/>
0164	<AttributeValue type="Enumeration" value="Compromised"/>
0165	</Attribute>
0166	</ResponsePayload>
0167	</BatchItem>
0168	</ResponseMessage>
	# TIME 4
0169	<RequestMessage>
0170	<RequestHeader>
0171	<ProtocolVersion>
0172	<ProtocolVersionMajor type="Integer" value="1"/>
0173	<ProtocolVersionMinor type="Integer" value="1"/>
0174	</ProtocolVersion>
0175	<BatchCount type="Integer" value="1"/>
0176	</RequestHeader>
0177	<BatchItem>
0178	<Operation type="Enumeration" value="ReKey"/>
0179	<RequestPayload>
0180	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0181	</RequestPayload>
0182	</BatchItem>
0183	</RequestMessage>
0184	<ResponseMessage>
0185	<ResponseHeader>
0186	<ProtocolVersion>
0187	<ProtocolVersionMajor type="Integer" value="1"/>
0188	<ProtocolVersionMinor type="Integer" value="1"/>
0189	</ProtocolVersion>
0190	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0191	<BatchCount type="Integer" value="1"/>
0192	</ResponseHeader>

0193	<BatchItem>
0194	<Operation type="Enumeration" value="ReKey"/>
0195	<ResultStatus type="Enumeration" value="Success"/>
0196	<ResponsePayload>
0197	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0198	</ResponsePayload>
0199	</BatchItem>
0200	</ResponseMessage>
# TIME 5	
0201	<RequestMessage>
0202	<RequestHeader>
0203	<ProtocolVersion>
0204	<ProtocolVersionMajor type="Integer" value="1"/>
0205	<ProtocolVersionMinor type="Integer" value="1"/>
0206	</ProtocolVersion>
0207	<BatchCount type="Integer" value="1"/>
0208	</RequestHeader>
0209	<BatchItem>
0210	<Operation type="Enumeration" value="GetAttributes"/>
0211	<RequestPayload>
0212	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0213	<AttributeName type="TextString" value="State"/>
0214	</RequestPayload>
0215	</BatchItem>
0216	</RequestMessage>
0217	<ResponseMessage>
0218	<ResponseHeader>
0219	<ProtocolVersion>
0220	<ProtocolVersionMajor type="Integer" value="1"/>
0221	<ProtocolVersionMinor type="Integer" value="1"/>
0222	</ProtocolVersion>
0223	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0224	<BatchCount type="Integer" value="1"/>
0225	</ResponseHeader>
0226	<BatchItem>
0227	<Operation type="Enumeration" value="GetAttributes"/>
0228	<ResultStatus type="Enumeration" value="Success"/>
0229	<ResponsePayload>
0230	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0231	<Attribute>
0232	<AttributeName type="TextString" value="State"/>
0233	<AttributeValue type="Enumeration" value="Active"/>
0234	</Attribute>
0235	</ResponsePayload>
0236	</BatchItem>
0237	</ResponseMessage>
# TIME 6	
0238	<RequestMessage>
0239	<RequestHeader>
0240	<ProtocolVersion>
0241	<ProtocolVersionMajor type="Integer" value="1"/>
0242	<ProtocolVersionMinor type="Integer" value="1"/>
0243	</ProtocolVersion>

0244	<BatchCount type="Integer" value="1"/>
0245	</RequestHeader>
0246	<BatchItem>
0247	<Operation type="Enumeration" value="Destroy"/>
0248	<RequestPayload>
0249	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0250	</RequestPayload>
0251	</BatchItem>
0252	</RequestMessage>
0253	<ResponseMessage>
0254	<ResponseHeader>
0255	<ProtocolVersion>
0256	<ProtocolVersionMajor type="Integer" value="1"/>
0257	<ProtocolVersionMinor type="Integer" value="1"/>
0258	</ProtocolVersion>
0259	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0260	<BatchCount type="Integer" value="1"/>
0261	</ResponseHeader>
0262	<BatchItem>
0263	<Operation type="Enumeration" value="Destroy"/>
0264	<ResultStatus type="Enumeration" value="Success"/>
0265	<ResponsePayload>
0266	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0267	</ResponsePayload>
0268	</BatchItem>
0269	</ResponseMessage>
	# TIME 7
0270	<RequestMessage>
0271	<RequestHeader>
0272	<ProtocolVersion>
0273	<ProtocolVersionMajor type="Integer" value="1"/>
0274	<ProtocolVersionMinor type="Integer" value="1"/>
0275	</ProtocolVersion>
0276	<BatchOrderOption type="Boolean" value="true"/>
0277	<BatchCount type="Integer" value="2"/>
0278	</RequestHeader>
0279	<BatchItem>
0280	<Operation type="Enumeration" value="Revoke"/>
0281	<UniqueBatchItemID type="ByteString" value="c95bbfd6ad466474"/>
0282	<RequestPayload>
0283	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0284	<RevocationReason>
0285	<RevocationReasonCode type="Enumeration"
	value="CessationOfOperation"/>
0286	</RevocationReason>
0287	</RequestPayload>
0288	</BatchItem>
0289	<BatchItem>
0290	<Operation type="Enumeration" value="Destroy"/>
0291	<UniqueBatchItemID type="ByteString" value="4e6a3e943e1dda87"/>
0292	<RequestPayload>
0293	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0294	</RequestPayload>

0295	</BatchItem>
0296	</RequestMessage>
0297	<ResponseMessage>
0298	<ResponseHeader>
0299	<ProtocolVersion>
0300	<ProtocolVersionMajor type="Integer" value="1"/>
0301	<ProtocolVersionMinor type="Integer" value="1"/>
0302	</ProtocolVersion>
0303	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0304	<BatchCount type="Integer" value="2"/>
0305	</ResponseHeader>
0306	<BatchItem>
0307	<Operation type="Enumeration" value="Revoke"/>
0308	<UniqueBatchItemID type="ByteString" value="c95bbfd6ad466474"/>
0309	<ResultStatus type="Enumeration" value="Success"/>
0310	<ResponsePayload>
0311	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0312	</ResponsePayload>
0313	</BatchItem>
0314	<BatchItem>
0315	<Operation type="Enumeration" value="Destroy"/>
0316	<UniqueBatchItemID type="ByteString" value="4e6a3e943e1dda87"/>
0317	<ResultStatus type="Enumeration" value="Success"/>
0318	<ResponsePayload>
0319	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0320	</ResponsePayload>
0321	</BatchItem>
0322	</ResponseMessage>

439

440 2.2.17 TC-94-11 - Create Key, Re-key with New Life-cycle

441 Create a symmetric key with a specific name, then use Locate to find the key. After using Re-key
442 to create a new key, verify that the name was removed from the existing key and copied to the
443 new key. To clean up, both keys are deleted.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>

0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="TC-94-11-rekeyKey"/>
0030	<NameType type="Enumeration" value="UninterpretedTextString"/>
0031	</AttributeValue>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="1"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
	# TIME 1
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="1"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="Locate"/>
0065	<RequestPayload>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Name"/>
0068	<AttributeValue>

0069	<NameValue type="TextString" value="TC-94-11-rekeyKey"/>
0070	<NameType type="Enumeration"
0071	value="UninterpretedTextString"/>
0072	</AttributeValue>
0073	</Attribute>
0074	</RequestPayload>
0075	</BatchItem>
0076	</RequestMessage>
0077	<ResponseMessage>
0078	<ResponseHeader>
0079	<ProtocolVersion>
0080	<ProtocolVersionMajor type="Integer" value="1"/>
0081	<ProtocolVersionMinor type="Integer" value="1"/>
0082	</ProtocolVersion>
0083	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0084	<BatchCount type="Integer" value="1"/>
0085	</ResponseHeader>
0086	<BatchItem>
0087	<Operation type="Enumeration" value="Locate"/>
0088	<ResultStatus type="Enumeration" value="Success"/>
0089	<ResponsePayload>
0090	<UniqueIdentifier type="TextString"
0091	value="\$UNIQUE_IDENTIFIER_0"/>
0092	</ResponsePayload>
0093	</BatchItem>
0094	</ResponseMessage>
0095	# TIME 2
0096	<RequestMessage>
0097	<RequestHeader>
0098	<ProtocolVersion>
0099	<ProtocolVersionMajor type="Integer" value="1"/>
0100	<ProtocolVersionMinor type="Integer" value="1"/>
0101	</ProtocolVersion>
0102	<BatchCount type="Integer" value="1"/>
0103	</RequestHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="ReKey"/>
0106	<RequestPayload>
0107	<UniqueIdentifier type="TextString"
0108	value="\$UNIQUE_IDENTIFIER_0"/>
0109	<TemplateAttribute>
0110	<Attribute>
0111	<AttributeName type="TextString" value="Activation Date"/>
0112	<AttributeValue type="DateTime" value="\$NOW-31536000"/>
0113	</Attribute>
0114	<Attribute>
0115	<AttributeName type="TextString" value="Process Start
0116	Date"/>
0117	<AttributeValue type="DateTime" value="\$NOW-31536000"/>
0118	</Attribute>
0119	<Attribute>
0120	<AttributeName type="TextString" value="Protect Stop
0121	Date"/>
0122	<AttributeValue type="DateTime" value="\$NOW+31536000"/>
0123	</Attribute>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Deactivation

0120	Date"/>
0121	<AttributeValue type="DateTime" value="\$NOW+31536000"/>
0122	</Attribute>
0123	</TemplateAttribute>
0124	</RequestPayload>
0125	</BatchItem>
0126	</RequestMessage>
0127	<ResponseMessage>
0128	<ResponseHeader>
0129	<ProtocolVersion>
0130	<ProtocolVersionMajor type="Integer" value="1"/>
0131	<ProtocolVersionMinor type="Integer" value="1"/>
0132	</ProtocolVersion>
0133	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0134	<BatchCount type="Integer" value="1"/>
0135	</ResponseHeader>
0136	<BatchItem>
0137	<Operation type="Enumeration" value="ReKey"/>
0138	<ResultStatus type="Enumeration" value="Success"/>
0139	<ResponsePayload>
0140	<UniqueIdentifier type="TextString"
0141	value="\$UNIQUE_IDENTIFIER_1"/>
0142	</ResponsePayload>
0143	</BatchItem>
0144	</ResponseMessage>
0145	# TIME 3
0146	<RequestMessage>
0147	<RequestHeader>
0148	<ProtocolVersion>
0149	<ProtocolVersionMajor type="Integer" value="1"/>
0150	<ProtocolVersionMinor type="Integer" value="1"/>
0151	</ProtocolVersion>
0152	<BatchCount type="Integer" value="1"/>
0153	</RequestHeader>
0154	<BatchItem>
0155	<Operation type="Enumeration" value="GetAttributes"/>
0156	<RequestPayload>
0157	<UniqueIdentifier type="TextString"
0158	value="\$UNIQUE_IDENTIFIER_0"/>
0159	<AttributeName type="TextString" value="Name"/>
0160	</RequestPayload>
0161	</BatchItem>
0162	</RequestMessage>
0163	<ResponseMessage>
0164	<ResponseHeader>
0165	<ProtocolVersion>
0166	<ProtocolVersionMajor type="Integer" value="1"/>
0167	<ProtocolVersionMinor type="Integer" value="1"/>
0168	</ProtocolVersion>
0169	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0170	<BatchCount type="Integer" value="1"/>
0171	</ResponseHeader>
	<BatchItem>
	<Operation type="Enumeration" value="GetAttributes"/>
	<ResultStatus type="Enumeration" value="Success"/>
	<ResponsePayload>

0172	<UniqueIdentifier type="TextString"
0173	value="\$UNIQUE_IDENTIFIER_0"/>
0174	</ResponsePayload>
0175	</BatchItem>
	</ResponseMessage>
	# TIME 4
0176	<RequestMessage>
0177	<RequestHeader>
0178	<ProtocolVersion>
0179	<ProtocolVersionMajor type="Integer" value="1"/>
0180	<ProtocolVersionMinor type="Integer" value="1"/>
0181	</ProtocolVersion>
0182	<BatchCount type="Integer" value="1"/>
0183	</RequestHeader>
0184	<BatchItem>
0185	<Operation type="Enumeration" value="GetAttributes"/>
0186	<RequestPayload>
0187	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0188	<AttributeName type="TextString" value="Activation Date"/>
0189	<AttributeName type="TextString" value="Process Start Date"/>
0190	<AttributeName type="TextString" value="Protect Stop Date"/>
0191	<AttributeName type="TextString" value="Deactivation Date"/>
0192	</RequestPayload>
0193	</BatchItem>
0194	</RequestMessage>
0195	<ResponseMessage>
0196	<ResponseHeader>
0197	<ProtocolVersion>
0198	<ProtocolVersionMajor type="Integer" value="1"/>
0199	<ProtocolVersionMinor type="Integer" value="1"/>
0200	</ProtocolVersion>
0201	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0202	<BatchCount type="Integer" value="1"/>
0203	</ResponseHeader>
0204	<BatchItem>
0205	<Operation type="Enumeration" value="GetAttributes"/>
0206	<ResultStatus type="Enumeration" value="Success"/>
0207	<ResponsePayload>
0208	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0209	<Attribute>
0210	<AttributeName type="TextString" value="Activation Date"/>
0211	<AttributeValue type="DateTime" value="\$NOW-31536000"/>
0212	</Attribute>
0213	<Attribute>
0214	<AttributeName type="TextString" value="Process Start
	Date"/>
0215	<AttributeValue type="DateTime" value="\$NOW-31536000"/>
0216	</Attribute>
0217	<Attribute>
0218	<AttributeName type="TextString" value="Protect Stop Date"/>
0219	<AttributeValue type="DateTime" value="\$NOW+31536000"/>
0220	</Attribute>
0221	<Attribute>
0222	<AttributeName type="TextString" value="Deactivation Date"/>
0223	<AttributeValue type="DateTime" value="\$NOW+31536000"/>

0224	</Attribute>
0225	</ResponsePayload>
0226	</BatchItem>
0227	</ResponseMessage>
# TIME 5	
0228	<RequestMessage>
0229	<RequestHeader>
0230	<ProtocolVersion>
0231	<ProtocolVersionMajor type="Integer" value="1"/>
0232	<ProtocolVersionMinor type="Integer" value="1"/>
0233	</ProtocolVersion>
0234	<BatchCount type="Integer" value="1"/>
0235	</RequestHeader>
0236	<BatchItem>
0237	<Operation type="Enumeration" value="Locate"/>
0238	<RequestPayload>
0239	<Attribute>
0240	<AttributeName type="TextString" value="Name"/>
0241	<AttributeValue>
0242	<NameValue type="TextString" value="TC-94-11-rekeyKey"/>
0243	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0244	</AttributeValue>
0245	</Attribute>
0246	</RequestPayload>
0247	</BatchItem>
0248	</RequestMessage>
0249	<ResponseMessage>
0250	<ResponseHeader>
0251	<ProtocolVersion>
0252	<ProtocolVersionMajor type="Integer" value="1"/>
0253	<ProtocolVersionMinor type="Integer" value="1"/>
0254	</ProtocolVersion>
0255	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0256	<BatchCount type="Integer" value="1"/>
0257	</ResponseHeader>
0258	<BatchItem>
0259	<Operation type="Enumeration" value="Locate"/>
0260	<ResultStatus type="Enumeration" value="Success"/>
0261	<ResponsePayload>
0262	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0263	</ResponsePayload>
0264	</BatchItem>
0265	</ResponseMessage>
# TIME 6	
0266	<RequestMessage>
0267	<RequestHeader>
0268	<ProtocolVersion>
0269	<ProtocolVersionMajor type="Integer" value="1"/>
0270	<ProtocolVersionMinor type="Integer" value="1"/>
0271	</ProtocolVersion>
0272	<BatchCount type="Integer" value="1"/>
0273	</RequestHeader>
0274	<BatchItem>
0275	<Operation type="Enumeration" value="Destroy"/>

0276	<RequestPayload>
0277	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0278	</RequestPayload>
0279	</BatchItem>
0280	</RequestMessage>
0281	<ResponseMessage>
0282	<ResponseHeader>
0283	<ProtocolVersion>
0284	<ProtocolVersionMajor type="Integer" value="1"/>
0285	<ProtocolVersionMinor type="Integer" value="1"/>
0286	</ProtocolVersion>
0287	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0288	<BatchCount type="Integer" value="1"/>
0289	</ResponseHeader>
0290	<BatchItem>
0291	<Operation type="Enumeration" value="Destroy"/>
0292	<ResultStatus type="Enumeration" value="Success"/>
0293	<ResponsePayload>
0294	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0295	</ResponsePayload>
0296	</BatchItem>
0297	</ResponseMessage>
	# TIME 7
0298	<RequestMessage>
0299	<RequestHeader>
0300	<ProtocolVersion>
0301	<ProtocolVersionMajor type="Integer" value="1"/>
0302	<ProtocolVersionMinor type="Integer" value="1"/>
0303	</ProtocolVersion>
0304	<BatchOrderOption type="Boolean" value="true"/>
0305	<BatchCount type="Integer" value="2"/>
0306	</RequestHeader>
0307	<BatchItem>
0308	<Operation type="Enumeration" value="Revoke"/>
0309	<UniqueBatchItemID type="ByteString" value="64bf984d81eee045"/>
0310	<RequestPayload>
0311	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0312	<RevocationReason>
0313	<RevocationReasonCode type="Enumeration"
	value="CessationOfOperation"/>
0314	</RevocationReason>
0315	</RequestPayload>
0316	</BatchItem>
0317	<BatchItem>
0318	<Operation type="Enumeration" value="Destroy"/>
0319	<UniqueBatchItemID type="ByteString" value="6e140354775e324d"/>
0320	<RequestPayload>
0321	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0322	</RequestPayload>
0323	</BatchItem>
0324	</RequestMessage>
0325	<ResponseMessage>

```

0326 <ResponseHeader>
0327   <ProtocolVersion>
0328     <ProtocolVersionMajor type="Integer" value="1"/>
0329     <ProtocolVersionMinor type="Integer" value="1"/>
0330   </ProtocolVersion>
0331   <TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0332   <BatchCount type="Integer" value="2"/>
0333 </ResponseHeader>
0334 <BatchItem>
0335   <Operation type="Enumeration" value="Revoke"/>
0336   <UniqueBatchItemID type="ByteString" value="64bf984d81eee045"/>
0337   <ResultStatus type="Enumeration" value="Success"/>
0338   <ResponsePayload>
0339     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0340   </ResponsePayload>
0341 </BatchItem>
0342 <BatchItem>
0343   <Operation type="Enumeration" value="Destroy"/>
0344   <UniqueBatchItemID type="ByteString" value="6e140354775e324d"/>
0345   <ResultStatus type="Enumeration" value="Success"/>
0346   <ResponsePayload>
0347     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0348   </ResponsePayload>
0349 </BatchItem>
0350 </ResponseMessage>

```

444

445 2.2.18 TC-95-11 - Obtain Lease for Expired Key

446 Create a symmetric key with a specific name and obtain a lease. Revoke the key with state
447 'Compromised' and re-key the key. Try to obtain a lease on the old key which fails due to a
448 server policy which does not allow giving out leases for compromised keys. Locate the new key
449 with the original name. Get the new key and obtain a lease.

```

# TIME 0
# [Client-A]
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="1"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="Create"/>
0011     <RequestPayload>
0012       <ObjectType type="Enumeration" value="SymmetricKey"/>
0013       <TemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0016           <AttributeValue type="Enumeration" value="AES"/>

```

0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="TC-95-11-rekeyKey"/>
0030	<NameType type="Enumeration" value="UninterpretedTextString"/>
0031	</AttributeValue>
0032	</Attribute>
0033	<Attribute>
0034	<AttributeName type="TextString" value="Activation Date"/>
0035	<AttributeValue type="DateTime" value="\$NOW"/>
0036	</Attribute>
0037	</TemplateAttribute>
0038	</RequestPayload>
0039	</BatchItem>
0040	</RequestMessage>
0041	<ResponseMessage>
0042	<ResponseHeader>
0043	<ProtocolVersion>
0044	<ProtocolVersionMajor type="Integer" value="1"/>
0045	<ProtocolVersionMinor type="Integer" value="1"/>
0046	</ProtocolVersion>
0047	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0048	<BatchCount type="Integer" value="1"/>
0049	</ResponseHeader>
0050	<BatchItem>
0051	<Operation type="Enumeration" value="Create"/>
0052	<ResultStatus type="Enumeration" value="Success"/>
0053	<ResponsePayload>
0054	<ObjectType type="Enumeration" value="SymmetricKey"/>
0055	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0056	</ResponsePayload>
0057	</BatchItem>
0058	</ResponseMessage>
	# TIME 1
	# [Client-A]
0059	<RequestMessage>
0060	<RequestHeader>
0061	<ProtocolVersion>
0062	<ProtocolVersionMajor type="Integer" value="1"/>
0063	<ProtocolVersionMinor type="Integer" value="1"/>
0064	</ProtocolVersion>
0065	<BatchCount type="Integer" value="1"/>
0066	</RequestHeader>
0067	<BatchItem>

0068	<Operation type="Enumeration" value="Get"/>
0069	<RequestPayload>
0070	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0071	</RequestPayload>
0072	</BatchItem>
0073	</RequestMessage>
0074	<ResponseMessage>
0075	<ResponseHeader>
0076	<ProtocolVersion>
0077	<ProtocolVersionMajor type="Integer" value="1"/>
0078	<ProtocolVersionMinor type="Integer" value="1"/>
0079	</ProtocolVersion>
0080	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0081	<BatchCount type="Integer" value="1"/>
0082	</ResponseHeader>
0083	<BatchItem>
0084	<Operation type="Enumeration" value="Get"/>
0085	<ResultStatus type="Enumeration" value="Success"/>
0086	<ResponsePayload>
0087	<ObjectType type="Enumeration" value="SymmetricKey"/>
0088	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0089	<SymmetricKey>
0090	<KeyBlock>
0091	<KeyFormatType type="Enumeration" value="Raw"/>
0092	<KeyValue>
0093	<KeyMaterial type="ByteString"
	value="ef5a0e97a29b32034c66efbf26ad3e42"/>
0094	</KeyValue>
0095	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0096	<CryptographicLength type="Integer" value="128"/>
0097	</KeyBlock>
0098	</SymmetricKey>
0099	</ResponsePayload>
0100	</BatchItem>
0101	</ResponseMessage>
	# TIME 2
	# [Client-A]
0102	<RequestMessage>
0103	<RequestHeader>
0104	<ProtocolVersion>
0105	<ProtocolVersionMajor type="Integer" value="1"/>
0106	<ProtocolVersionMinor type="Integer" value="1"/>
0107	</ProtocolVersion>
0108	<BatchCount type="Integer" value="1"/>
0109	</RequestHeader>
0110	<BatchItem>
0111	<Operation type="Enumeration" value="ObtainLease"/>
0112	<RequestPayload>
0113	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0114	</RequestPayload>
0115	</BatchItem>
0116	</RequestMessage>
0117	<ResponseMessage>

0118	<ResponseHeader>
0119	<ProtocolVersion>
0120	<ProtocolVersionMajor type="Integer" value="1"/>
0121	<ProtocolVersionMinor type="Integer" value="1"/>
0122	</ProtocolVersion>
0123	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0124	<BatchCount type="Integer" value="1"/>
0125	</ResponseHeader>
0126	<BatchItem>
0127	<Operation type="Enumeration" value="ObtainLease"/>
0128	<ResultStatus type="Enumeration" value="Success"/>
0129	<ResponsePayload>
0130	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0131	<LeaseTime type="Interval" value="0"/>
0132	<LastChangeDate type="DateTime" value="\$NOW"/>
0133	</ResponsePayload>
0134	</BatchItem>
0135	</ResponseMessage>
	# TIME 3
	# [Client-B]
0136	<RequestMessage>
0137	<RequestHeader>
0138	<ProtocolVersion>
0139	<ProtocolVersionMajor type="Integer" value="1"/>
0140	<ProtocolVersionMinor type="Integer" value="1"/>
0141	</ProtocolVersion>
0142	<BatchCount type="Integer" value="1"/>
0143	</RequestHeader>
0144	<BatchItem>
0145	<Operation type="Enumeration" value="Revoke"/>
0146	<RequestPayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0148	<RevocationReason>
0149	<RevocationReasonCode type="Enumeration"
	value="KeyCompromise"/>
0150	</RevocationReason>
0151	<CompromiseOccurrenceDate type="DateTime" value="\$NOW"/>
0152	</RequestPayload>
0153	</BatchItem>
0154	</RequestMessage>
0155	<ResponseMessage>
0156	<ResponseHeader>
0157	<ProtocolVersion>
0158	<ProtocolVersionMajor type="Integer" value="1"/>
0159	<ProtocolVersionMinor type="Integer" value="1"/>
0160	</ProtocolVersion>
0161	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0162	<BatchCount type="Integer" value="1"/>
0163	</ResponseHeader>
0164	<BatchItem>
0165	<Operation type="Enumeration" value="Revoke"/>
0166	<ResultStatus type="Enumeration" value="Success"/>
0167	<ResponsePayload>
0168	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0169	</ResponsePayload>
0170	</BatchItem>
0171	</ResponseMessage>
	# TIME 4
	# [Client-B]
0172	<RequestMessage>
0173	<RequestHeader>
0174	<ProtocolVersion>
0175	<ProtocolVersionMajor type="Integer" value="1"/>
0176	<ProtocolVersionMinor type="Integer" value="1"/>
0177	</ProtocolVersion>
0178	<BatchCount type="Integer" value="1"/>
0179	</RequestHeader>
0180	<BatchItem>
0181	<Operation type="Enumeration" value="ReKey"/>
0182	<RequestPayload>
0183	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0184	</RequestPayload>
0185	</BatchItem>
0186	</RequestMessage>
0187	<ResponseMessage>
0188	<ResponseHeader>
0189	<ProtocolVersion>
0190	<ProtocolVersionMajor type="Integer" value="1"/>
0191	<ProtocolVersionMinor type="Integer" value="1"/>
0192	</ProtocolVersion>
0193	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0194	<BatchCount type="Integer" value="1"/>
0195	</ResponseHeader>
0196	<BatchItem>
0197	<Operation type="Enumeration" value="ReKey"/>
0198	<ResultStatus type="Enumeration" value="Success"/>
0199	<ResponsePayload>
0200	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0201	</ResponsePayload>
0202	</BatchItem>
0203	</ResponseMessage>
	# TIME 5
	# [Client-A]
0204	<RequestMessage>
0205	<RequestHeader>
0206	<ProtocolVersion>
0207	<ProtocolVersionMajor type="Integer" value="1"/>
0208	<ProtocolVersionMinor type="Integer" value="1"/>
0209	</ProtocolVersion>
0210	<BatchCount type="Integer" value="1"/>
0211	</RequestHeader>
0212	<BatchItem>
0213	<Operation type="Enumeration" value="ObtainLease"/>
0214	<RequestPayload>
0215	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0216	</RequestPayload>
0217	</BatchItem>

0218	</RequestMessage>
0219	<ResponseMessage>
0220	<ResponseHeader>
0221	<ProtocolVersion>
0222	<ProtocolVersionMajor type="Integer" value="1"/>
0223	<ProtocolVersionMinor type="Integer" value="1"/>
0224	</ProtocolVersion>
0225	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0226	<BatchCount type="Integer" value="1"/>
0227	</ResponseHeader>
0228	<BatchItem>
0229	<Operation type="Enumeration" value="ObtainLease"/>
0230	<ResultStatus type="Enumeration" value="OperationFailed"/>
0231	<ResultReason type="Enumeration" value="PermissionDenied"/>
0232	<ResultMessage type="TextString" value="CO is in state Compromised, no lease given"/>
0233	</BatchItem>
0234	</ResponseMessage>
# TIME 6 # [Client-A]	
0235	<RequestMessage>
0236	<RequestHeader>
0237	<ProtocolVersion>
0238	<ProtocolVersionMajor type="Integer" value="1"/>
0239	<ProtocolVersionMinor type="Integer" value="1"/>
0240	</ProtocolVersion>
0241	<BatchCount type="Integer" value="1"/>
0242	</RequestHeader>
0243	<BatchItem>
0244	<Operation type="Enumeration" value="Locate"/>
0245	<RequestPayload>
0246	<Attribute>
0247	<AttributeName type="TextString" value="Name"/>
0248	<AttributeValue>
0249	<NameValue type="TextString" value="TC-95-11-rekeyKey"/>
0250	<NameType type="Enumeration" value="UninterpretedTextString"/>
0251	</AttributeValue>
0252	</Attribute>
0253	</RequestPayload>
0254	</BatchItem>
0255	</RequestMessage>
0256	<ResponseMessage>
0257	<ResponseHeader>
0258	<ProtocolVersion>
0259	<ProtocolVersionMajor type="Integer" value="1"/>
0260	<ProtocolVersionMinor type="Integer" value="1"/>
0261	</ProtocolVersion>
0262	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0263	<BatchCount type="Integer" value="1"/>
0264	</ResponseHeader>
0265	<BatchItem>
0266	<Operation type="Enumeration" value="Locate"/>
0267	<ResultStatus type="Enumeration" value="Success"/>
0268	<ResponsePayload>
0269	<UniqueIdentifier type="TextString"

0270	value="\$UNIQUE_IDENTIFIER_1"/>
0271	</ResponsePayload>
0272	</BatchItem>
0272	</ResponseMessage>
	# TIME 7
	# [Client-A]
0273	<RequestMessage>
0274	<RequestHeader>
0275	<ProtocolVersion>
0276	<ProtocolVersionMajor type="Integer" value="1"/>
0277	<ProtocolVersionMinor type="Integer" value="1"/>
0278	</ProtocolVersion>
0279	<BatchCount type="Integer" value="1"/>
0280	</RequestHeader>
0281	<BatchItem>
0282	<Operation type="Enumeration" value="Get"/>
0283	<RequestPayload>
0284	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0285	</RequestPayload>
0286	</BatchItem>
0287	</RequestMessage>
0288	<ResponseMessage>
0289	<ResponseHeader>
0290	<ProtocolVersion>
0291	<ProtocolVersionMajor type="Integer" value="1"/>
0292	<ProtocolVersionMinor type="Integer" value="1"/>
0293	</ProtocolVersion>
0294	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0295	<BatchCount type="Integer" value="1"/>
0296	</ResponseHeader>
0297	<BatchItem>
0298	<Operation type="Enumeration" value="Get"/>
0299	<ResultStatus type="Enumeration" value="Success"/>
0300	<ResponsePayload>
0301	<ObjectType type="Enumeration" value="SymmetricKey"/>
0302	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0303	<SymmetricKey>
0304	<KeyBlock>
0305	<KeyFormatType type="Enumeration" value="Raw"/>
0306	<KeyValue>
0307	<KeyMaterial type="ByteString"
	value="525d4b0bbb66bcb538029d49a6f569a5"/>
0308	</KeyValue>
0309	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0310	<CryptographicLength type="Integer" value="128"/>
0311	</KeyBlock>
0312	</SymmetricKey>
0313	</ResponsePayload>
0314	</BatchItem>
0315	</ResponseMessage>
	# TIME 8
	# [Client-A]
0316	<RequestMessage>
0317	<RequestHeader>

0318	<ProtocolVersion>
0319	<ProtocolVersionMajor type="Integer" value="1"/>
0320	<ProtocolVersionMinor type="Integer" value="1"/>
0321	</ProtocolVersion>
0322	<BatchCount type="Integer" value="1"/>
0323	</RequestHeader>
0324	<BatchItem>
0325	<Operation type="Enumeration" value="ObtainLease"/>
0326	<RequestPayload>
0327	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0328	</RequestPayload>
0329	</BatchItem>
0330	</RequestMessage>
0331	<ResponseMessage>
0332	<ResponseHeader>
0333	<ProtocolVersion>
0334	<ProtocolVersionMajor type="Integer" value="1"/>
0335	<ProtocolVersionMinor type="Integer" value="1"/>
0336	</ProtocolVersion>
0337	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0338	<BatchCount type="Integer" value="1"/>
0339	</ResponseHeader>
0340	<BatchItem>
0341	<Operation type="Enumeration" value="ObtainLease"/>
0342	<ResultStatus type="Enumeration" value="Success"/>
0343	<ResponsePayload>
0344	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0345	<LeaseTime type="Interval" value="0"/>
0346	<LastChangeDate type="DateTime" value="\$NOW"/>
0347	</ResponsePayload>
0348	</BatchItem>
0349	</ResponseMessage>
	# TIME 9
	# [Client-A]
0350	<RequestMessage>
0351	<RequestHeader>
0352	<ProtocolVersion>
0353	<ProtocolVersionMajor type="Integer" value="1"/>
0354	<ProtocolVersionMinor type="Integer" value="1"/>
0355	</ProtocolVersion>
0356	<BatchCount type="Integer" value="1"/>
0357	</RequestHeader>
0358	<BatchItem>
0359	<Operation type="Enumeration" value="Destroy"/>
0360	<RequestPayload>
0361	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0362	</RequestPayload>
0363	</BatchItem>
0364	</RequestMessage>
0365	<ResponseMessage>
0366	<ResponseHeader>
0367	<ProtocolVersion>
0368	<ProtocolVersionMajor type="Integer" value="1"/>

0369	<ProtocolVersionMinor type="Integer" value="1"/>
0370	</ProtocolVersion>
0371	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0372	<BatchCount type="Integer" value="1"/>
0373	</ResponseHeader>
0374	<BatchItem>
0375	<Operation type="Enumeration" value="Destroy"/>
0376	<ResultStatus type="Enumeration" value="Success"/>
0377	<ResponsePayload>
0378	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0379	</ResponsePayload>
0380	</BatchItem>
0381	</ResponseMessage>
	# TIME 10
	# [Client-A]
0382	<RequestMessage>
0383	<RequestHeader>
0384	<ProtocolVersion>
0385	<ProtocolVersionMajor type="Integer" value="1"/>
0386	<ProtocolVersionMinor type="Integer" value="1"/>
0387	</ProtocolVersion>
0388	<BatchOrderOption type="Boolean" value="true"/>
0389	<BatchCount type="Integer" value="2"/>
0390	</RequestHeader>
0391	<BatchItem>
0392	<Operation type="Enumeration" value="Revoke"/>
0393	<UniqueBatchItemID type="ByteString" value="e00004346ea64da4"/>
0394	<RequestPayload>
0395	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0396	<RevocationReason>
0397	<RevocationReasonCode type="Enumeration"
	value="CessationOfOperation"/>
0398	</RevocationReason>
0399	</RequestPayload>
0400	</BatchItem>
0401	<BatchItem>
0402	<Operation type="Enumeration" value="Destroy"/>
0403	<UniqueBatchItemID type="ByteString" value="0376ca8cdcc8a2f1"/>
0404	<RequestPayload>
0405	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0406	</RequestPayload>
0407	</BatchItem>
0408	</RequestMessage>
0409	<ResponseMessage>
0410	<ResponseHeader>
0411	<ProtocolVersion>
0412	<ProtocolVersionMajor type="Integer" value="1"/>
0413	<ProtocolVersionMinor type="Integer" value="1"/>
0414	</ProtocolVersion>
0415	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0416	<BatchCount type="Integer" value="2"/>
0417	</ResponseHeader>
0418	<BatchItem>
0419	<Operation type="Enumeration" value="Revoke"/>

0420	<UniqueBatchItemID type="ByteString" value="e00004346ea64da4"/>
0421	<ResultStatus type="Enumeration" value="Success"/>
0422	<ResponsePayload>
0423	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0424	</ResponsePayload>
0425	</BatchItem>
0426	<BatchItem>
0427	<Operation type="Enumeration" value="Destroy"/>
0428	<UniqueBatchItemID type="ByteString" value="0376ca8cdcc8a2f1"/>
0429	<ResultStatus type="Enumeration" value="Success"/>
0430	<ResponsePayload>
0431	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0432	</ResponsePayload>
0433	</BatchItem>
0434	</ResponseMessage>

450

451 2.2.19 TC-101-11 - Create a Key, Archive and Recover it

452 Create a symmetric key with a specified name, then use Locate to find the key and get the key.
453 Archive the key (asynchronous operation, use Poll until it completes) and use Get and Locate on
454 it, but both fail (Get returns an error and Locate returns no Unique Identifiers). Add the Storage
455 Status Mask to the Locate-command, indicating to the server to search in both online and
456 archived storage. The Locate then finds the archived key. Recover the key (asynchronous
457 operation, use Poll until it completes) from the archive, then repeat the Get operation which will
458 now succeed.

459 Since the client is unable to force the server to respond asynchronously, it is possible for a
460 server to respond synchronously to the requests issued at times 3 and 9, in which case the
461 expected responses are the ones shown at times 4 and 10 respectively.

462 Note: a server may perform Archive and Recover operations synchronously and not require the
463 use of Poll for the client to wait for the operation to complete

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>

0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="TC-101-11- archiveKey"/>
0030	<NameType type="Enumeration" value="UninterpretedTextString"/>
0031	</AttributeValue>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="1"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
0055	# TIME 1 <RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="1"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="Locate"/>
0065	<RequestPayload>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Object Type"/>

0068	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Name"/>
0072	<AttributeValue>
0073	<NameValue type="TextString" value="TC-101-11- archiveKey"/>
0074	<NameType type="Enumeration" value="UninterpretedTextString"/>
0075	</AttributeValue>
0076	</Attribute>
0077	</RequestPayload>
0078	</BatchItem>
0079	</RequestMessage>
0080	<ResponseMessage>
0081	<ResponseHeader>
0082	<ProtocolVersion>
0083	<ProtocolVersionMajor type="Integer" value="1"/>
0084	<ProtocolVersionMinor type="Integer" value="1"/>
0085	</ProtocolVersion>
0086	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0087	<BatchCount type="Integer" value="1"/>
0088	</ResponseHeader>
0089	<BatchItem>
0090	<Operation type="Enumeration" value="Locate"/>
0091	<ResultStatus type="Enumeration" value="Success"/>
0092	<ResponsePayload>
0093	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0094	</ResponsePayload>
0095	</BatchItem>
0096	</ResponseMessage>
	# TIME 2
0097	<RequestMessage>
0098	<RequestHeader>
0099	<ProtocolVersion>
0100	<ProtocolVersionMajor type="Integer" value="1"/>
0101	<ProtocolVersionMinor type="Integer" value="1"/>
0102	</ProtocolVersion>
0103	<BatchCount type="Integer" value="1"/>
0104	</RequestHeader>
0105	<BatchItem>
0106	<Operation type="Enumeration" value="Get"/>
0107	<RequestPayload>
0108	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0109	</RequestPayload>
0110	</BatchItem>
0111	</RequestMessage>
0112	<ResponseMessage>
0113	<ResponseHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="1"/>
0117	</ProtocolVersion>
0118	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>

0119	<BatchCount type="Integer" value="1"/>
0120	</ResponseHeader>
0121	<BatchItem>
0122	<Operation type="Enumeration" value="Get"/>
0123	<ResultStatus type="Enumeration" value="Success"/>
0124	<ResponsePayload>
0125	<ObjectType type="Enumeration" value="SymmetricKey"/>
0126	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0127	<SymmetricKey>
0128	<KeyBlock>
0129	<KeyFormatType type="Enumeration" value="Raw"/>
0130	<KeyValue>
0131	<KeyMaterial type="ByteString"
	value="0b4c9fb659c5ce09ec12c3233d526f45"/>
0132	</KeyValue>
0133	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0134	<CryptographicLength type="Integer" value="128"/>
0135	</KeyBlock>
0136	</SymmetricKey>
0137	</ResponsePayload>
0138	</BatchItem>
0139	</ResponseMessage>
# TIME 3	
0140	<RequestMessage>
0141	<RequestHeader>
0142	<ProtocolVersion>
0143	<ProtocolVersionMajor type="Integer" value="1"/>
0144	<ProtocolVersionMinor type="Integer" value="1"/>
0145	</ProtocolVersion>
0146	<AsynchronousIndicator type="Boolean" value="true"/>
0147	<BatchCount type="Integer" value="1"/>
0148	</RequestHeader>
0149	<BatchItem>
0150	<Operation type="Enumeration" value="Archive"/>
0151	<RequestPayload>
0152	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0153	</RequestPayload>
0154	</BatchItem>
0155	</RequestMessage>
0156	<ResponseMessage>
0157	<ResponseHeader>
0158	<ProtocolVersion>
0159	<ProtocolVersionMajor type="Integer" value="1"/>
0160	<ProtocolVersionMinor type="Integer" value="1"/>
0161	</ProtocolVersion>
0162	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0163	<BatchCount type="Integer" value="1"/>
0164	</ResponseHeader>
0165	<BatchItem>
0166	<Operation type="Enumeration" value="Archive"/>
0167	<ResultStatus type="Enumeration" value="OperationPending"/>
0168	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0169	</BatchItem>
0170	</ResponseMessage>

0171	# TIME 4
0172	# [REPEAT] until Archive response is returned
0173	<RequestMessage>
0174	<RequestHeader>
0175	<ProtocolVersion>
0176	<ProtocolVersionMajor type="Integer" value="1"/>
0177	<ProtocolVersionMinor type="Integer" value="1"/>
0178	</ProtocolVersion>
0179	<BatchCount type="Integer" value="1"/>
0180	</BatchCount>
0181	<Operation type="Enumeration" value="Poll"/>
0182	<RequestPayload>
0183	<AsynchronousCorrelationValue type="ByteString"
0184	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0185	</RequestPayload>
0186	</BatchItem>
0187	</RequestMessage>
0188	<ResponseMessage>
0189	<ResponseHeader>
0190	<ProtocolVersion>
0191	<ProtocolVersionMajor type="Integer" value="1"/>
0192	<ProtocolVersionMinor type="Integer" value="1"/>
0193	</ProtocolVersion>
0194	<TimeStamp type="DateTime" value="2012-04-27T08:14:30+00:00"/>
0195	<BatchCount type="Integer" value="1"/>
0196	</BatchCount>
0197	<Operation type="Enumeration" value="Archive"/>
0198	<ResultStatus type="Enumeration" value="Success"/>
0199	<ResponsePayload>
0200	<UniqueIdentifier type="TextString"
0201	value="\$UNIQUE_IDENTIFIER_0"/>
0202	</ResponsePayload>
0203	</BatchItem>
0204	</ResponseMessage>
0205	# TIME 5
0206	<RequestMessage>
0207	<RequestHeader>
0208	<ProtocolVersion>
0209	<ProtocolVersionMajor type="Integer" value="1"/>
0210	<ProtocolVersionMinor type="Integer" value="1"/>
0211	</ProtocolVersion>
0212	<BatchCount type="Integer" value="1"/>
0213	</BatchCount>
0214	<Operation type="Enumeration" value="Get"/>
0215	<RequestPayload>
0216	<UniqueIdentifier type="TextString"
0217	value="\$UNIQUE_IDENTIFIER_0"/>
0218	</RequestPayload>
0219	</BatchItem>
0220	</RequestMessage>
0221	<ResponseMessage>
0222	<ResponseHeader>
0223	<ProtocolVersion>

0221	<ProtocolVersionMajor type="Integer" value="1"/>
0222	<ProtocolVersionMinor type="Integer" value="1"/>
0223	</ProtocolVersion>
0224	<TimeStamp type="DateTime" value="2012-04-27T08:14:32+00:00"/>
0225	<BatchCount type="Integer" value="1"/>
0226	</ResponseHeader>
0227	<BatchItem>
0228	<Operation type="Enumeration" value="Get"/>
0229	<ResultStatus type="Enumeration" value="OperationFailed"/>
0230	<ResultReason type="Enumeration" value="ObjectArchived"/>
0231	<ResultMessage type="TextString" value="Object is archived"/>
0232	</BatchItem>
0233	</ResponseMessage>
# TIME 6	
0234	<RequestMessage>
0235	<RequestHeader>
0236	<ProtocolVersion>
0237	<ProtocolVersionMajor type="Integer" value="1"/>
0238	<ProtocolVersionMinor type="Integer" value="1"/>
0239	</ProtocolVersion>
0240	<BatchCount type="Integer" value="1"/>
0241	</RequestHeader>
0242	<BatchItem>
0243	<Operation type="Enumeration" value="GetAttributes"/>
0244	<RequestPayload>
0245	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0246	<AttributeName type="TextString" value="Archive Date"/>
0247	</RequestPayload>
0248	</BatchItem>
0249	</RequestMessage>
0250	<ResponseMessage>
0251	<ResponseHeader>
0252	<ProtocolVersion>
0253	<ProtocolVersionMajor type="Integer" value="1"/>
0254	<ProtocolVersionMinor type="Integer" value="1"/>
0255	</ProtocolVersion>
0256	<TimeStamp type="DateTime" value="2012-04-27T08:14:32+00:00"/>
0257	<BatchCount type="Integer" value="1"/>
0258	</ResponseHeader>
0259	<BatchItem>
0260	<Operation type="Enumeration" value="GetAttributes"/>
0261	<ResultStatus type="Enumeration" value="Success"/>
0262	<ResponsePayload>
0263	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0264	<Attribute>
0265	<AttributeName type="TextString" value="Archive Date"/>
0266	<AttributeValue type="DateTime" value="2012-04-
	27T08:14:30+00:00"/>
0267	</Attribute>
0268	</ResponsePayload>
0269	</BatchItem>
0270	</ResponseMessage>
# TIME 7	
0271	<RequestMessage>

0272	<RequestHeader>
0273	<ProtocolVersion>
0274	<ProtocolVersionMajor type="Integer" value="1"/>
0275	<ProtocolVersionMinor type="Integer" value="1"/>
0276	</ProtocolVersion>
0277	<BatchCount type="Integer" value="1"/>
0278	</RequestHeader>
0279	<BatchItem>
0280	<Operation type="Enumeration" value="Locate"/>
0281	<RequestPayload>
0282	<Attribute>
0283	<AttributeName type="TextString" value="Object Type"/>
0284	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0285	</Attribute>
0286	<Attribute>
0287	<AttributeName type="TextString" value="Name"/>
0288	<AttributeValue>
0289	<NameValue type="TextString" value="TC-101-11-
0290	archiveKey"/>
0291	<NameType type="Enumeration"
0292	value="UninterpretedTextString"/>
0293	</AttributeValue>
0294	</Attribute>
0295	</RequestPayload>
0296	</BatchItem>
0297	</RequestMessage>
0298	<ResponseMessage>
0299	<ResponseHeader>
0300	<ProtocolVersion>
0301	<ProtocolVersionMajor type="Integer" value="1"/>
0302	<ProtocolVersionMinor type="Integer" value="1"/>
0303	</ProtocolVersion>
0304	<TimeStamp type="DateTime" value="2012-04-27T08:14:33+00:00"/>
0305	<BatchCount type="Integer" value="1"/>
0306	</ResponseHeader>
0307	<BatchItem>
0308	<Operation type="Enumeration" value="Locate"/>
0309	<ResultStatus type="Enumeration" value="Success"/>
0310	<ResponsePayload>
0311	</BatchItem>
0312	</ResponseMessage>
0313	# TIME 8
0314	<RequestMessage>
0315	<RequestHeader>
0316	<ProtocolVersion>
0317	<ProtocolVersionMajor type="Integer" value="1"/>
0318	<ProtocolVersionMinor type="Integer" value="1"/>
0319	</ProtocolVersion>
0320	<BatchCount type="Integer" value="1"/>
0321	</RequestHeader>
0322	<BatchItem>
0323	<Operation type="Enumeration" value="Locate"/>
0324	<RequestPayload>
	<StorageStatusMask type="Integer" value="ArchivalStorage
	OnLineStorage"/>
	<Attribute>

0325	<AttributeName type="TextString" value="Object Type"/>
0326	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0327	</Attribute>
0328	<Attribute>
0329	<AttributeName type="TextString" value="Name"/>
0330	<AttributeValue>
0331	<NameValue type="TextString" value="TC-101-11- archiveKey"/>
0332	<NameType type="Enumeration" value="UninterpretedTextString"/>
0333	</AttributeValue>
0334	</Attribute>
0335	</RequestPayload>
0336	</BatchItem>
0337	</RequestMessage>
0338	<ResponseMessage>
0339	<ResponseHeader>
0340	<ProtocolVersion>
0341	<ProtocolVersionMajor type="Integer" value="1"/>
0342	<ProtocolVersionMinor type="Integer" value="1"/>
0343	</ProtocolVersion>
0344	<TimeStamp type="DateTime" value="2012-04-27T08:14:33+00:00"/>
0345	<BatchCount type="Integer" value="1"/>
0346	</ResponseHeader>
0347	<BatchItem>
0348	<Operation type="Enumeration" value="Locate"/>
0349	<ResultStatus type="Enumeration" value="Success"/>
0350	<ResponsePayload>
0351	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0352	</ResponsePayload>
0353	</BatchItem>
0354	</ResponseMessage>
# TIME 9	
0355	<RequestMessage>
0356	<RequestHeader>
0357	<ProtocolVersion>
0358	<ProtocolVersionMajor type="Integer" value="1"/>
0359	<ProtocolVersionMinor type="Integer" value="1"/>
0360	</ProtocolVersion>
0361	<AsynchronousIndicator type="Boolean" value="true"/>
0362	<BatchCount type="Integer" value="1"/>
0363	</RequestHeader>
0364	<BatchItem>
0365	<Operation type="Enumeration" value="Recover"/>
0366	<RequestPayload>
0367	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0368	</RequestPayload>
0369	</BatchItem>
0370	</RequestMessage>
0371	<ResponseMessage>
0372	<ResponseHeader>
0373	<ProtocolVersion>
0374	<ProtocolVersionMajor type="Integer" value="1"/>
0375	<ProtocolVersionMinor type="Integer" value="1"/>

0376	</ProtocolVersion>
0377	<TimeStamp type="DateTime" value="2012-04-27T08:14:33+00:00"/>
0378	<BatchCount type="Integer" value="1"/>
0379	</ResponseHeader>
0380	<BatchItem>
0381	<Operation type="Enumeration" value="Recover"/>
0382	<ResultStatus type="Enumeration" value="OperationPending"/>
0383	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0384	</BatchItem>
0385	</ResponseMessage>
	<i># TIME 10</i>
	<i># [REPEAT] until Recover response is returned</i>
0386	<RequestMessage>
0387	<RequestHeader>
0388	<ProtocolVersion>
0389	<ProtocolVersionMajor type="Integer" value="1"/>
0390	<ProtocolVersionMinor type="Integer" value="1"/>
0391	</ProtocolVersion>
0392	<BatchCount type="Integer" value="1"/>
0393	</RequestHeader>
0394	<BatchItem>
0395	<Operation type="Enumeration" value="Poll"/>
0396	<RequestPayload>
0397	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0398	</RequestPayload>
0399	</BatchItem>
0400	</RequestMessage>
0401	<ResponseMessage>
0402	<ResponseHeader>
0403	<ProtocolVersion>
0404	<ProtocolVersionMajor type="Integer" value="1"/>
0405	<ProtocolVersionMinor type="Integer" value="1"/>
0406	</ProtocolVersion>
0407	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0408	<BatchCount type="Integer" value="1"/>
0409	</ResponseHeader>
0410	<BatchItem>
0411	<Operation type="Enumeration" value="Recover"/>
0412	<ResultStatus type="Enumeration" value="Success"/>
0413	<ResponsePayload>
0414	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0415	</ResponsePayload>
0416	</BatchItem>
0417	</ResponseMessage>
	<i># TIME 11</i>
0418	<RequestMessage>
0419	<RequestHeader>
0420	<ProtocolVersion>
0421	<ProtocolVersionMajor type="Integer" value="1"/>
0422	<ProtocolVersionMinor type="Integer" value="1"/>
0423	</ProtocolVersion>
0424	<BatchCount type="Integer" value="1"/>
0425	</RequestHeader>

0426	<BatchItem>
0427	<Operation type="Enumeration" value="Get"/>
0428	<RequestPayload>
0429	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0430	</RequestPayload>
0431	</BatchItem>
0432	</RequestMessage>
0433	<ResponseMessage>
0434	<ResponseHeader>
0435	<ProtocolVersion>
0436	<ProtocolVersionMajor type="Integer" value="1"/>
0437	<ProtocolVersionMinor type="Integer" value="1"/>
0438	</ProtocolVersion>
0439	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0440	<BatchCount type="Integer" value="1"/>
0441	</ResponseHeader>
0442	<BatchItem>
0443	<Operation type="Enumeration" value="Get"/>
0444	<ResultStatus type="Enumeration" value="Success"/>
0445	<ResponsePayload>
0446	<ObjectType type="Enumeration" value="SymmetricKey"/>
0447	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0448	<SymmetricKey>
0449	<KeyBlock>
0450	<KeyFormatType type="Enumeration" value="Raw"/>
0451	<KeyValue>
0452	<KeyMaterial type="ByteString"
	value="0b4c9fb659c5ce09ec12c3233d526f45"/>
0453	</KeyValue>
0454	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0455	<CryptographicLength type="Integer" value="128"/>
0456	</KeyBlock>
0457	</SymmetricKey>
0458	</ResponsePayload>
0459	</BatchItem>
0460	</ResponseMessage>
	# TIME 12
0461	<RequestMessage>
0462	<RequestHeader>
0463	<ProtocolVersion>
0464	<ProtocolVersionMajor type="Integer" value="1"/>
0465	<ProtocolVersionMinor type="Integer" value="1"/>
0466	</ProtocolVersion>
0467	<BatchCount type="Integer" value="1"/>
0468	</RequestHeader>
0469	<BatchItem>
0470	<Operation type="Enumeration" value="Destroy"/>
0471	<RequestPayload>
0472	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0473	</RequestPayload>
0474	</BatchItem>
0475	</RequestMessage>
0476	<ResponseMessage>

```
0477 <ResponseHeader>
0478   <ProtocolVersion>
0479     <ProtocolVersionMajor type="Integer" value="1"/>
0480     <ProtocolVersionMinor type="Integer" value="1"/>
0481   </ProtocolVersion>
0482   <TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0483   <BatchCount type="Integer" value="1"/>
0484 </ResponseHeader>
0485 <BatchItem>
0486   <Operation type="Enumeration" value="Destroy"/>
0487   <ResultStatus type="Enumeration" value="Success"/>
0488   <ResponsePayload>
0489     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0490   </ResponsePayload>
0491 </BatchItem>
0492 </ResponseMessage>
```

464

465 2.2.20 TC-111-11 - Credential, Operation Policy, Destroy Date

466 Pass a Credential object of type Username and Password in the message header in all requests
467 for identification purposes. Create a symmetric key and set the Operation Policy Name attribute
468 to 'default'. Using another Username and Password Credential, attempt to perform a Get
469 operation batched with a Get Attribute List on the created symmetric key - according to the
470 Default Operation Policy, both these request SHALL fail, and with the Batch Error Continuation
471 Option set to 'Continue', the client SHALL also receive both response payloads. Using the first
472 (correct) Credential, Destroy the object and then get the Destroy Date attribute.

473 The message exchanges shown in this test case assume that the first Credential (Fred) is valid
474 and the second credential (Barney) is either invalid or does not have access to the newly created
475 key (which should always be true under the 'default' Operation Policy).

476 Note: a server can elect to not return meta-data for destroyed objects and in those
477 circumstances the Get Attributes operation may fail.

```
# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="1"/>
0006     </ProtocolVersion>
0007     <Authentication>
0008       <Credential>
0009         <CredentialType type="Enumeration"
value="UsernameAndPassword"/>
0010         <CredentialValue>
0011           <Username type="TextString" value="Fred"/>
0012           <Password type="TextString" value="password1"/>
0013         </CredentialValue>
0014       </Credential>
0015     </Authentication>
0016     <BatchCount type="Integer" value="1"/>
```

0017	</RequestHeader>
0018	<BatchItem>
0019	<Operation type="Enumeration" value="Create"/>
0020	<RequestPayload>
0021	<ObjectType type="Enumeration" value="SymmetricKey"/>
0022	<TemplateAttribute>
0023	<Attribute>
0024	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0025	<AttributeValue type="Enumeration" value="AES"/>
0026	</Attribute>
0027	<Attribute>
0028	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0029	<AttributeValue type="Integer" value="128"/>
0030	</Attribute>
0031	<Attribute>
0032	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0033	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0034	</Attribute>
0035	<Attribute>
0036	<AttributeName type="TextString" value="Name"/>
0037	<AttributeValue>
0038	<NameValue type="TextString" value="TC-111-11-key1"/>
0039	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0040	</AttributeValue>
0041	</Attribute>
0042	<Attribute>
0043	<AttributeName type="TextString" value="Operation Policy
	Name"/>
0044	<AttributeValue type="TextString" value="default"/>
0045	</Attribute>
0046	<Attribute>
0047	<AttributeName type="TextString" value="Cryptographic
	Parameters"/>
0048	<AttributeValue>
0049	<BlockCipherMode type="Enumeration" value="CBC"/>
0050	<PaddingMethod type="Enumeration" value="PKCS5"/>
0051	<HashingAlgorithm type="Enumeration" value="SHA_1"/>
0052	</AttributeValue>
0053	</Attribute>
0054	</TemplateAttribute>
0055	</RequestPayload>
0056	</BatchItem>
0057	</RequestMessage>
0058	<ResponseMessage>
0059	<ResponseHeader>
0060	<ProtocolVersion>
0061	<ProtocolVersionMajor type="Integer" value="1"/>
0062	<ProtocolVersionMinor type="Integer" value="1"/>
0063	</ProtocolVersion>
0064	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0065	<BatchCount type="Integer" value="1"/>
0066	</ResponseHeader>
0067	<BatchItem>

0068	<Operation type="Enumeration" value="Create"/>
0069	<ResultStatus type="Enumeration" value="Success"/>
0070	<ResponsePayload>
0071	<ObjectType type="Enumeration" value="SymmetricKey"/>
0072	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0073	</ResponsePayload>
0074	</BatchItem>
0075	</ResponseMessage>
	# TIME 1
0076	<RequestMessage>
0077	<RequestHeader>
0078	<ProtocolVersion>
0079	<ProtocolVersionMajor type="Integer" value="1"/>
0080	<ProtocolVersionMinor type="Integer" value="1"/>
0081	</ProtocolVersion>
0082	<Authentication>
0083	<Credential>
0084	<CredentialType type="Enumeration"
	value="UsernameAndPassword"/>
0085	<CredentialValue>
0086	<Username type="TextString" value="Fred"/>
0087	<Password type="TextString" value="password1"/>
0088	</CredentialValue>
0089	</Credential>
0090	</Authentication>
0091	<BatchCount type="Integer" value="2"/>
0092	</RequestHeader>
0093	<BatchItem>
0094	<Operation type="Enumeration" value="GetAttributes"/>
0095	<UniqueBatchItemID type="ByteString" value="55d88770e2556dab"/>
0096	<RequestPayload>
0097	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0098	<AttributeName type="TextString" value="Operation Policy
	Name"/>
0099	</RequestPayload>
0100	</BatchItem>
0101	<BatchItem>
0102	<Operation type="Enumeration" value="Get"/>
0103	<UniqueBatchItemID type="ByteString" value="eb864ee01f1f98cd"/>
0104	<RequestPayload>
0105	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0106	</RequestPayload>
0107	</BatchItem>
0108	</RequestMessage>
0109	<ResponseMessage>
0110	<ResponseHeader>
0111	<ProtocolVersion>
0112	<ProtocolVersionMajor type="Integer" value="1"/>
0113	<ProtocolVersionMinor type="Integer" value="1"/>
0114	</ProtocolVersion>
0115	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0116	<BatchCount type="Integer" value="2"/>
0117	</ResponseHeader>
0118	<BatchItem>

0119	<Operation type="Enumeration" value="GetAttributes"/>
0120	<UniqueBatchItemID type="ByteString" value="55d88770e2556dab"/>
0121	<ResultStatus type="Enumeration" value="Success"/>
0122	<ResponsePayload>
0123	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Operation Policy
	Name"/>
0126	<AttributeValue type="TextString" value="default"/>
0127	</Attribute>
0128	</ResponsePayload>
0129	</BatchItem>
0130	<BatchItem>
0131	<Operation type="Enumeration" value="Get"/>
0132	<UniqueBatchItemID type="ByteString" value="eb864ee01f1f98cd"/>
0133	<ResultStatus type="Enumeration" value="Success"/>
0134	<ResponsePayload>
0135	<ObjectType type="Enumeration" value="SymmetricKey"/>
0136	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0137	<SymmetricKey>
0138	<KeyBlock>
0139	<KeyFormatType type="Enumeration" value="Raw"/>
0140	<KeyValue>
0141	<KeyMaterial type="ByteString"
	value="30e55f4b230b34ce8afc476c66f8351b"/>
0142	</KeyValue>
0143	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0144	<CryptographicLength type="Integer" value="128"/>
0145	</KeyBlock>
0146	</SymmetricKey>
0147	</ResponsePayload>
0148	</BatchItem>
0149	</ResponseMessage>
	# TIME 2
0150	<RequestMessage>
0151	<RequestHeader>
0152	<ProtocolVersion>
0153	<ProtocolVersionMajor type="Integer" value="1"/>
0154	<ProtocolVersionMinor type="Integer" value="1"/>
0155	</ProtocolVersion>
0156	<Authentication>
0157	<Credential>
0158	<CredentialType type="Enumeration"
	value="UsernameAndPassword"/>
0159	<CredentialValue>
0160	<Username type="TextString" value="Barney"/>
0161	<Password type="TextString" value="secret2"/>
0162	</CredentialValue>
0163	</Credential>
0164	</Authentication>
0165	<BatchErrorContinuationOption type="Enumeration"
	value="Continue"/>
0166	<BatchOrderOption type="Boolean" value="true"/>
0167	<BatchCount type="Integer" value="2"/>
0168	</RequestHeader>

0169	<BatchItem>
0170	<Operation type="Enumeration" value="Get"/>
0171	<UniqueBatchItemID type="ByteString" value="4f0e6d3dba3d0495"/>
0172	<RequestPayload>
0173	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0174	</RequestPayload>
0175	</BatchItem>
0176	<BatchItem>
0177	<Operation type="Enumeration" value="GetAttributeList"/>
0178	<UniqueBatchItemID type="ByteString" value="9b937e7cd50b233b"/>
0179	<RequestPayload>
0180	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0181	</RequestPayload>
0182	</BatchItem>
0183	</RequestMessage>
0184	<ResponseMessage>
0185	<ResponseHeader>
0186	<ProtocolVersion>
0187	<ProtocolVersionMajor type="Integer" value="1"/>
0188	<ProtocolVersionMinor type="Integer" value="1"/>
0189	</ProtocolVersion>
0190	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0191	<BatchCount type="Integer" value="2"/>
0192	</ResponseHeader>
0193	<BatchItem>
0194	<Operation type="Enumeration" value="Get"/>
0195	<UniqueBatchItemID type="ByteString" value="4f0e6d3dba3d0495"/>
0196	<ResultStatus type="Enumeration" value="OperationFailed"/>
0197	<ResultReason type="Enumeration" value="PermissionDenied"/>
0198	<ResultMessage type="TextString" value="Access denied"/>
0199	</BatchItem>
0200	<BatchItem>
0201	<Operation type="Enumeration" value="GetAttributeList"/>
0202	<UniqueBatchItemID type="ByteString" value="9b937e7cd50b233b"/>
0203	<ResultStatus type="Enumeration" value="OperationFailed"/>
0204	<ResultReason type="Enumeration" value="PermissionDenied"/>
0205	<ResultMessage type="TextString" value="Access denied"/>
0206	</BatchItem>
0207	</ResponseMessage>
	# TIME 3
0208	<RequestMessage>
0209	<RequestHeader>
0210	<ProtocolVersion>
0211	<ProtocolVersionMajor type="Integer" value="1"/>
0212	<ProtocolVersionMinor type="Integer" value="1"/>
0213	</ProtocolVersion>
0214	<Authentication>
0215	<Credential>
0216	<CredentialType type="Enumeration"
	value="UsernameAndPassword"/>
0217	<CredentialValue>
0218	<Username type="TextString" value="Fred"/>
0219	<Password type="TextString" value="password1"/>
0220	</CredentialValue>
0221	</Credential>

0222	</Authentication>
0223	<BatchCount type="Integer" value="1"/>
0224	</RequestHeader>
0225	<BatchItem>
0226	<Operation type="Enumeration" value="Destroy"/>
0227	<RequestPayload>
0228	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0229	</RequestPayload>
0230	</BatchItem>
0231	</RequestMessage>
0232	<ResponseMessage>
0233	<ResponseHeader>
0234	<ProtocolVersion>
0235	<ProtocolVersionMajor type="Integer" value="1"/>
0236	<ProtocolVersionMinor type="Integer" value="1"/>
0237	</ProtocolVersion>
0238	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0239	<BatchCount type="Integer" value="1"/>
0240	</ResponseHeader>
0241	<BatchItem>
0242	<Operation type="Enumeration" value="Destroy"/>
0243	<ResultStatus type="Enumeration" value="Success"/>
0244	<ResponsePayload>
0245	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0246	</ResponsePayload>
0247	</BatchItem>
0248	</ResponseMessage>
	# TIME 4
0249	<RequestMessage>
0250	<RequestHeader>
0251	<ProtocolVersion>
0252	<ProtocolVersionMajor type="Integer" value="1"/>
0253	<ProtocolVersionMinor type="Integer" value="1"/>
0254	</ProtocolVersion>
0255	<Authentication>
0256	<Credential>
0257	<CredentialType type="Enumeration"
	value="UsernameAndPassword"/>
0258	<CredentialValue>
0259	<Username type="TextString" value="Fred"/>
0260	<Password type="TextString" value="password1"/>
0261	</CredentialValue>
0262	</Credential>
0263	</Authentication>
0264	<BatchCount type="Integer" value="1"/>
0265	</RequestHeader>
0266	<BatchItem>
0267	<Operation type="Enumeration" value="GetAttributes"/>
0268	<RequestPayload>
0269	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0270	<AttributeName type="TextString" value="Destroy Date"/>
0271	</RequestPayload>
0272	</BatchItem>
0273	</RequestMessage>

```

0274 <ResponseMessage>
0275   <ResponseHeader>
0276     <ProtocolVersion>
0277       <ProtocolVersionMajor type="Integer" value="1"/>
0278       <ProtocolVersionMinor type="Integer" value="1"/>
0279     </ProtocolVersion>
0280     <TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0281     <BatchCount type="Integer" value="1"/>
0282   </ResponseHeader>
0283   <BatchItem>
0284     <Operation type="Enumeration" value="GetAttributes"/>
0285     <ResultStatus type="Enumeration" value="Success"/>
0286     <ResponsePayload>
0287       <UniqueIdentifier type="TextString"
0288       value="$UNIQUE_IDENTIFIER_0"/>
0289       <Attribute>
0289         <AttributeName type="TextString" value="Destroy Date"/>
0290         <AttributeValue type="DateTime" value="2012-04-
0291         27T08:14:35+00:00"/>
0291       </Attribute>
0292     </ResponsePayload>
0293   </BatchItem>
0294 </ResponseMessage>

```

478

479 2.2.21 TC-112-11 - Device Credential, Operation Policy, Destroy Date

480 Pass a Credential object of type Device Credential in the message header in all requests for
481 identification purposes. Create a symmetric key and set the Operation Policy Name attribute to
482 'default'. Using another Credential, attempt to perform a Get operation batched with a Get
483 Attribute List on the created symmetric key. According to the Default Operation Policy, both
484 these request SHALL fail, and with the Batch Error Continuation Option set to 'Continue', the
485 client SHALL also receive both response payloads. Using the first Credential, Destroy the object
486 and get the Destroy Date attribute. The message exchanges shown in this test case assume that
487 the first Credential (devID2233) is valid and the second credential (devID4444) is either invalid
488 or does not have access to the newly created key (which should always be true under the
489 'default' Operation Policy).

490 Note: a server can elect to not return meta-data for destroyed objects and in those
491 circumstances the Get Attributes operation may fail.

```

0001 # TIME 0
0002 <RequestMessage>
0003   <RequestHeader>
0004     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="1"/>
0006     </ProtocolVersion>
0007     <Authentication>
0008     <Credential>
0009       <CredentialType type="Enumeration" value="Device"/>
0010       <CredentialValue>
0011       <DeviceSerialNumber type="TextString"

```

```

0012 value="serNum123456"/>
0013     <Password type="TextString" value="secret"/>
0014     <DeviceIdentifier type="TextString" value="devID2233"/>
0015     <NetworkIdentifier type="TextString" value="netID9000"/>
0016     <MachineIdentifier type="TextString" value="machineID1"/>
0017     <MediaIdentifier type="TextString" value="mediaID313"/>
0018     </CredentialValue>
0019     </Credential>
0020     </Authentication>
0021     <BatchCount type="Integer" value="1"/>
0022 </RequestHeader>
0023 <BatchItem>
0024     <Operation type="Enumeration" value="Create"/>
0025     <RequestPayload>
0026         <ObjectType type="Enumeration" value="SymmetricKey"/>
0027         <TemplateAttribute>
0028             <Attribute>
0029                 <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0030                 <AttributeValue type="Enumeration" value="AES"/>
0031             </Attribute>
0032             <Attribute>
0033                 <AttributeName type="TextString" value="Cryptographic
Length"/>
0034                 <AttributeValue type="Integer" value="128"/>
0035             </Attribute>
0036             <Attribute>
0037                 <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0038                 <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0039             </Attribute>
0040             <Attribute>
0041                 <AttributeName type="TextString" value="Name"/>
0042                 <AttributeValue>
0043                     <NameValue type="TextString" value="TC-112-11-key1"/>
0044                     <NameType type="Enumeration"
value="UninterpretedTextString"/>
0045                 </AttributeValue>
0046             </Attribute>
0047             <Attribute>
0048                 <AttributeName type="TextString" value="Operation Policy
Name"/>
0049                 <AttributeValue type="TextString" value="default"/>
0050             </Attribute>
0051             <Attribute>
0052                 <AttributeName type="TextString" value="Cryptographic
Parameters"/>
0053                 <AttributeValue>
0054                     <BlockCipherMode type="Enumeration" value="CBC"/>
0055                     <PaddingMethod type="Enumeration" value="PKCS5"/>
0056                     <HashingAlgorithm type="Enumeration" value="SHA_1"/>
0057                 </AttributeValue>
0058             </Attribute>
0059         </TemplateAttribute>
0060     </RequestPayload>
0061 </BatchItem>
</RequestMessage>

```

0062	<ResponseMessage>
0063	<ResponseHeader>
0064	<ProtocolVersion>
0065	<ProtocolVersionMajor type="Integer" value="1"/>
0066	<ProtocolVersionMinor type="Integer" value="1"/>
0067	</ProtocolVersion>
0068	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0069	<BatchCount type="Integer" value="1"/>
0070	</ResponseHeader>
0071	<BatchItem>
0072	<Operation type="Enumeration" value="Create"/>
0073	<ResultStatus type="Enumeration" value="Success"/>
0074	<ResponsePayload>
0075	<ObjectType type="Enumeration" value="SymmetricKey"/>
0076	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0077	</ResponsePayload>
0078	</BatchItem>
0079	</ResponseMessage>
	# TIME 1
0080	<RequestMessage>
0081	<RequestHeader>
0082	<ProtocolVersion>
0083	<ProtocolVersionMajor type="Integer" value="1"/>
0084	<ProtocolVersionMinor type="Integer" value="1"/>
0085	</ProtocolVersion>
0086	<Authentication>
0087	<Credential>
0088	<CredentialType type="Enumeration" value="Device"/>
0089	<CredentialValue>
0090	<DeviceSerialNumber type="TextString"
	value="serNum123456"/>
0091	<Password type="TextString" value="secret"/>
0092	<DeviceIdentifier type="TextString" value="devID2233"/>
0093	<NetworkIdentifier type="TextString" value="netID9000"/>
0094	<MachineIdentifier type="TextString" value="machineID1"/>
0095	<MediaIdentifier type="TextString" value="mediaID313"/>
0096	</CredentialValue>
0097	</Credential>
0098	</Authentication>
0099	<BatchCount type="Integer" value="2"/>
0100	</RequestHeader>
0101	<BatchItem>
0102	<Operation type="Enumeration" value="GetAttributes"/>
0103	<UniqueBatchItemID type="ByteString" value="e705e27dc0ba7789"/>
0104	<RequestPayload>
0105	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0106	<AttributeName type="TextString" value="Operation Policy
	Name"/>
0107	</RequestPayload>
0108	</BatchItem>
0109	<BatchItem>
0110	<Operation type="Enumeration" value="Get"/>
0111	<UniqueBatchItemID type="ByteString" value="50a7f741a1119826"/>
0112	<RequestPayload>
0113	<UniqueIdentifier type="TextString"

0114	value="\$UNIQUE_IDENTIFIER_0"/>
0115	</RequestPayload>
0116	</BatchItem>
0117	</RequestMessage>
0117	<ResponseMessage>
0118	<ResponseHeader>
0119	<ProtocolVersion>
0120	<ProtocolVersionMajor type="Integer" value="1"/>
0121	<ProtocolVersionMinor type="Integer" value="1"/>
0122	</ProtocolVersion>
0123	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0124	<BatchCount type="Integer" value="2"/>
0125	</ResponseHeader>
0126	<BatchItem>
0127	<Operation type="Enumeration" value="GetAttributes"/>
0128	<UniqueBatchItemID type="ByteString" value="e705e27dc0ba7789"/>
0129	<ResultStatus type="Enumeration" value="Success"/>
0130	<ResponsePayload>
0131	<UniqueIdentifier type="TextString"
0132	value="\$UNIQUE_IDENTIFIER_0"/>
0132	<Attribute>
0133	<AttributeName type="TextString" value="Operation Policy
0134	Name"/>
0134	<AttributeValue type="TextString" value="default"/>
0135	</Attribute>
0136	</ResponsePayload>
0137	</BatchItem>
0138	<BatchItem>
0139	<Operation type="Enumeration" value="Get"/>
0140	<UniqueBatchItemID type="ByteString" value="50a7f741a1119826"/>
0141	<ResultStatus type="Enumeration" value="Success"/>
0142	<ResponsePayload>
0143	<ObjectType type="Enumeration" value="SymmetricKey"/>
0144	<UniqueIdentifier type="TextString"
0145	value="\$UNIQUE_IDENTIFIER_0"/>
0145	<SymmetricKey>
0146	<KeyBlock>
0147	<KeyFormatType type="Enumeration" value="Raw"/>
0148	<KeyValue>
0149	<KeyMaterial type="ByteString"
0150	value="acfeaffdbdd17d0e63624a22083ee4b6"/>
0150	</KeyValue>
0151	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0152	<CryptographicLength type="Integer" value="128"/>
0153	</KeyBlock>
0154	</SymmetricKey>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
	# TIME 2
0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="1"/>
0163	</ProtocolVersion>
0164	<Authentication>

0165	<Credential>
0166	<CredentialType type="Enumeration" value="Device"/>
0167	<CredentialValue>
0168	<DeviceSerialNumber type="TextString"
	value="serNum101010"/>
0169	<Password type="TextString" value="passwd"/>
0170	<DeviceIdentifier type="TextString" value="devID4444"/>
0171	<NetworkIdentifier type="TextString" value="netID9"/>
0172	<MachineIdentifier type="TextString"
	value="machineID1111"/>
0173	<MediaIdentifier type="TextString" value="mediaID0000"/>
0174	</CredentialValue>
0175	</Credential>
0176	</Authentication>
0177	<BatchErrorContinuationOption type="Enumeration"
	value="Continue"/>
0178	<BatchOrderOption type="Boolean" value="true"/>
0179	<BatchCount type="Integer" value="2"/>
0180	</RequestHeader>
0181	<BatchItem>
0182	<Operation type="Enumeration" value="Get"/>
0183	<UniqueBatchItemID type="ByteString" value="1154049d742c498e"/>
0184	<RequestPayload>
0185	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0186	</RequestPayload>
0187	</BatchItem>
0188	<BatchItem>
0189	<Operation type="Enumeration" value="GetAttributeList"/>
0190	<UniqueBatchItemID type="ByteString" value="8ae55c6e91d97b05"/>
0191	<RequestPayload>
0192	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0193	</RequestPayload>
0194	</BatchItem>
0195	</RequestMessage>
0196	<ResponseMessage>
0197	<ResponseHeader>
0198	<ProtocolVersion>
0199	<ProtocolVersionMajor type="Integer" value="1"/>
0200	<ProtocolVersionMinor type="Integer" value="1"/>
0201	</ProtocolVersion>
0202	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0203	<BatchCount type="Integer" value="2"/>
0204	</ResponseHeader>
0205	<BatchItem>
0206	<Operation type="Enumeration" value="Get"/>
0207	<UniqueBatchItemID type="ByteString" value="1154049d742c498e"/>
0208	<ResultStatus type="Enumeration" value="OperationFailed"/>
0209	<ResultReason type="Enumeration" value="PermissionDenied"/>
0210	<ResultMessage type="TextString" value="Access denied"/>
0211	</BatchItem>
0212	<BatchItem>
0213	<Operation type="Enumeration" value="GetAttributeList"/>
0214	<UniqueBatchItemID type="ByteString" value="8ae55c6e91d97b05"/>
0215	<ResultStatus type="Enumeration" value="OperationFailed"/>
0216	<ResultReason type="Enumeration" value="PermissionDenied"/>

0217	<ResultMessage type="TextString" value="Access denied"/>
0218	</BatchItem>
0219	</ResponseMessage>
# TIME 3	
0220	<RequestMessage>
0221	<RequestHeader>
0222	<ProtocolVersion>
0223	<ProtocolVersionMajor type="Integer" value="1"/>
0224	<ProtocolVersionMinor type="Integer" value="1"/>
0225	</ProtocolVersion>
0226	<Authentication>
0227	<Credential>
0228	<CredentialType type="Enumeration" value="Device"/>
0229	<CredentialValue>
0230	<DeviceSerialNumber type="TextString"
	value="serNum123456"/>
0231	<Password type="TextString" value="secret"/>
0232	<DeviceIdentifier type="TextString" value="devID2233"/>
0233	<NetworkIdentifier type="TextString" value="netID9000"/>
0234	<MachineIdentifier type="TextString" value="machineID1"/>
0235	<MediaIdentifier type="TextString" value="mediaID313"/>
0236	</CredentialValue>
0237	</Credential>
0238	</Authentication>
0239	<BatchCount type="Integer" value="1"/>
0240	</RequestHeader>
0241	<BatchItem>
0242	<Operation type="Enumeration" value="Destroy"/>
0243	<RequestPayload>
0244	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0245	</RequestPayload>
0246	</BatchItem>
0247	</RequestMessage>
0248	<ResponseMessage>
0249	<ResponseHeader>
0250	<ProtocolVersion>
0251	<ProtocolVersionMajor type="Integer" value="1"/>
0252	<ProtocolVersionMinor type="Integer" value="1"/>
0253	</ProtocolVersion>
0254	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0255	<BatchCount type="Integer" value="1"/>
0256	</ResponseHeader>
0257	<BatchItem>
0258	<Operation type="Enumeration" value="Destroy"/>
0259	<ResultStatus type="Enumeration" value="Success"/>
0260	<ResponsePayload>
0261	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0262	</ResponsePayload>
0263	</BatchItem>
0264	</ResponseMessage>
# TIME 4	
0265	<RequestMessage>
0266	<RequestHeader>
0267	<ProtocolVersion>

0268	<ProtocolVersionMajor type="Integer" value="1"/>
0269	<ProtocolVersionMinor type="Integer" value="1"/>
0270	</ProtocolVersion>
0271	<Authentication>
0272	<Credential>
0273	<CredentialType type="Enumeration" value="Device"/>
0274	<CredentialValue>
0275	<DeviceSerialNumber type="TextString"
	value="serNum123456"/>
0276	<Password type="TextString" value="secret"/>
0277	<DeviceIdentifier type="TextString" value="devID2233"/>
0278	<NetworkIdentifier type="TextString" value="netID9000"/>
0279	<MachineIdentifier type="TextString" value="machineID1"/>
0280	<MediaIdentifier type="TextString" value="mediaID313"/>
0281	</CredentialValue>
0282	</Credential>
0283	</Authentication>
0284	<BatchCount type="Integer" value="1"/>
0285	</RequestHeader>
0286	<BatchItem>
0287	<Operation type="Enumeration" value="GetAttributes"/>
0288	<RequestPayload>
0289	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0290	<AttributeName type="TextString" value="Destroy Date"/>
0291	</RequestPayload>
0292	</BatchItem>
0293	</RequestMessage>
0294	<ResponseMessage>
0295	<ResponseHeader>
0296	<ProtocolVersion>
0297	<ProtocolVersionMajor type="Integer" value="1"/>
0298	<ProtocolVersionMinor type="Integer" value="1"/>
0299	</ProtocolVersion>
0300	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0301	<BatchCount type="Integer" value="1"/>
0302	</ResponseHeader>
0303	<BatchItem>
0304	<Operation type="Enumeration" value="GetAttributes"/>
0305	<ResultStatus type="Enumeration" value="Success"/>
0306	<ResponsePayload>
0307	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0308	<Attribute>
0309	<AttributeName type="TextString" value="Destroy Date"/>
0310	<AttributeValue type="DateTime" value="2012-04-
	27T08:14:35+00:00"/>
0311	</Attribute>
0312	</ResponsePayload>
0313	</BatchItem>
0314	</ResponseMessage>

493 2.2.22 TC-121-11 - Query, Maximum Response Size

494 Perform a Query operation, querying the Operations and Objects supported by the server, with
495 a restriction on the Maximum Response Size set in the request header. Since the resulting Query
496 response is too large, an error is returned. Increase the Maximum Response Size, resubmit the
497 Query request, and get a successful response.

498 Note: the list of object types supported and operations will vary depending on the server
499 implementation. The server can report the Vendor Identification in whatever TextString form
500 the vendor selects. The server may return vendor specific tags in the Server Information
501 structure indicating additional vendor-specific information about the server.

0001	# TIME 0
0002	<RequestMessage>
0003	<RequestHeader>
0004	<ProtocolVersion>
0005	<ProtocolVersionMajor type="Integer" value="1"/>
0006	<ProtocolVersionMinor type="Integer" value="1"/>
0007	</ProtocolVersion>
0008	<MaximumResponseSize type="Integer" value="256"/>
0009	<BatchCount type="Integer" value="1"/>
0010	</RequestHeader>
0011	<BatchItem>
0012	<Operation type="Enumeration" value="Query"/>
0013	<RequestPayload>
0014	<QueryFunction type="Enumeration" value="QueryOperations"/>
0015	<QueryFunction type="Enumeration" value="QueryObjects"/>
0016	</RequestPayload>
0017	</BatchItem>
0018	</RequestMessage>
0019	<ResponseMessage>
0020	<ResponseHeader>
0021	<ProtocolVersion>
0022	<ProtocolVersionMajor type="Integer" value="1"/>
0023	<ProtocolVersionMinor type="Integer" value="1"/>
0024	</ProtocolVersion>
0025	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0026	<BatchCount type="Integer" value="1"/>
0027	</ResponseHeader>
0028	<BatchItem>
0029	<Operation type="Enumeration" value="Query"/>
0030	<ResultStatus type="Enumeration" value="OperationFailed"/>
0031	<ResultReason type="Enumeration" value="ResponseTooLarge"/>
0032	<ResultMessage type="TextString" value="Response size: 648, Maximum Response Size indicated in request: 256"/>
0033	</BatchItem>
0034	</ResponseMessage>
0035	# TIME 1
0036	<RequestMessage>
0037	<RequestHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="1"/>
	</ProtocolVersion>
	<MaximumResponseSize type="Integer" value="2048"/>

0041	<BatchCount type="Integer" value="1"/>
0042	</RequestHeader>
0043	<BatchItem>
0044	<Operation type="Enumeration" value="Query"/>
0045	<RequestPayload>
0046	<QueryFunction type="Enumeration" value="QueryOperations"/>
0047	<QueryFunction type="Enumeration" value="QueryObjects"/>
0048	<QueryFunction type="Enumeration"
	value="QueryServerInformation"/>
0049	</RequestPayload>
0050	</BatchItem>
0051	</RequestMessage>
0052	<ResponseMessage>
0053	<ResponseHeader>
0054	<ProtocolVersion>
0055	<ProtocolVersionMajor type="Integer" value="1"/>
0056	<ProtocolVersionMinor type="Integer" value="1"/>
0057	</ProtocolVersion>
0058	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0059	<BatchCount type="Integer" value="1"/>
0060	</ResponseHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Query"/>
0063	<ResultStatus type="Enumeration" value="Success"/>
0064	<ResponsePayload>
0065	<Operation type="Enumeration" value="Create"/>
0066	<Operation type="Enumeration" value="CreateKeyPair"/>
0067	<Operation type="Enumeration" value="Register"/>
0068	<Operation type="Enumeration" value="ReKey"/>
0069	<Operation type="Enumeration" value="Certify"/>
0070	<Operation type="Enumeration" value="ReCertify"/>
0071	<Operation type="Enumeration" value="Locate"/>
0072	<Operation type="Enumeration" value="Check"/>
0073	<Operation type="Enumeration" value="Get"/>
0074	<Operation type="Enumeration" value="GetAttributes"/>
0075	<Operation type="Enumeration" value="GetAttributeList"/>
0076	<Operation type="Enumeration" value="AddAttribute"/>
0077	<Operation type="Enumeration" value="ModifyAttribute"/>
0078	<Operation type="Enumeration" value="DeleteAttribute"/>
0079	<Operation type="Enumeration" value="ObtainLease"/>
0080	<Operation type="Enumeration" value="GetUsageAllocation"/>
0081	<Operation type="Enumeration" value="Activate"/>
0082	<Operation type="Enumeration" value="Revoke"/>
0083	<Operation type="Enumeration" value="Destroy"/>
0084	<Operation type="Enumeration" value="Archive"/>
0085	<Operation type="Enumeration" value="Recover"/>
0086	<Operation type="Enumeration" value="Query"/>
0087	<Operation type="Enumeration" value="Cancel"/>
0088	<Operation type="Enumeration" value="Poll"/>
0089	<Operation type="Enumeration" value="ReKeyKeyPair"/>
0090	<Operation type="Enumeration" value="DiscoverVersions"/>
0091	<ObjectType type="Enumeration" value="Certificate"/>
0092	<ObjectType type="Enumeration" value="SymmetricKey"/>
0093	<ObjectType type="Enumeration" value="PublicKey"/>
0094	<ObjectType type="Enumeration" value="PrivateKey"/>
0095	<ObjectType type="Enumeration" value="Template"/>
0096	<ObjectType type="Enumeration" value="SecretData"/>

0097	<VendorIdentification type="TextString" value="SOME-VENDOR-
0098	NAME"/>
0099	<ServerInformation>
0100	</ServerInformation>
0101	</ResponsePayload>
0102	</BatchItem>
0103	</ResponseMessage>

502

503 2.2.23 TC-122-11 - Query Vendor Extensions

504 Query the server for a list and map of vendor extension tags it recognizes.

505 Note: Extension Type is an Integer as there is no corresponding enumerated type for the Item
506 Type field.

507

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Query"/>
0011	<RequestPayload>
0012	<QueryFunction type="Enumeration" value="QueryExtensionList"/>
0013	</RequestPayload>
0014	</BatchItem>
0015	</RequestMessage>
0016	<ResponseMessage>
0017	<ResponseHeader>
0018	<ProtocolVersion>
0019	<ProtocolVersionMajor type="Integer" value="1"/>
0020	<ProtocolVersionMinor type="Integer" value="1"/>
0021	</ProtocolVersion>
0022	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0023	<BatchCount type="Integer" value="1"/>
0024	</ResponseHeader>
0025	<BatchItem>
0026	<Operation type="Enumeration" value="Query"/>
0027	<ResultStatus type="Enumeration" value="Success"/>
0028	<ResponsePayload>
0029	<ExtensionInformation>
0030	<ExtensionName type="TextString" value="ACME LOCATION"/>
0031	</ExtensionInformation>
0032	<ExtensionInformation>
0033	<ExtensionName type="TextString" value="ACME ZIP CODE"/>
0034	</ExtensionInformation>
0035	</ResponsePayload>
0036	</BatchItem>
0037	</ResponseMessage>

	# TIME 1
0038	<RequestMessage>
0039	<RequestHeader>
0040	<ProtocolVersion>
0041	<ProtocolVersionMajor type="Integer" value="1"/>
0042	<ProtocolVersionMinor type="Integer" value="1"/>
0043	</ProtocolVersion>
0044	<BatchCount type="Integer" value="1"/>
0045	</RequestHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Query"/>
0048	<RequestPayload>
0049	<QueryFunction type="Enumeration" value="QueryExtensionMap"/>
0050	</RequestPayload>
0051	</BatchItem>
0052	</RequestMessage>
0053	<ResponseMessage>
0054	<ResponseHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="1"/>
0058	</ProtocolVersion>
0059	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0060	<BatchCount type="Integer" value="1"/>
0061	</ResponseHeader>
0062	<BatchItem>
0063	<Operation type="Enumeration" value="Query"/>
0064	<ResultStatus type="Enumeration" value="Success"/>
0065	<ResponsePayload>
0066	<ExtensionInformation>
0067	<ExtensionName type="TextString" value="ACME LOCATION"/>
0068	<ExtensionTag type="Integer" value="5548545"/>
0069	<ExtensionType type="Integer" value="7"/>
0070	</ExtensionInformation>
0071	<ExtensionInformation>
0072	<ExtensionName type="TextString" value="ACME ZIP CODE"/>
0073	<ExtensionTag type="Integer" value="5548546"/>
0074	<ExtensionType type="Integer" value="2"/>
0075	</ExtensionInformation>
0076	</ResponsePayload>
0077	</BatchItem>
0078	</ResponseMessage>

508

509 2.2.24 TC-131-11 - Register an Asymmetric Key Pair in PKCS1 Format

510 Register a private key in the PKCS_1 key format, then register the corresponding public key, also
511 in PKCS_1 format, with the Link attribute pointing to the previously registered private key.
512 Thereafter add the Link attribute to the private key, and perform Locate operations to find the
513 public and private keys using the Link attribute. Get both the private and public keys in PKCS_1
514 key format, then destroy both the private and the public key.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>

```
0003     <ProtocolVersion>
0004         <ProtocolVersionMajor type="Integer" value="1"/>
0005         <ProtocolVersionMinor type="Integer" value="1"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008 </RequestHeader>
0009 <BatchItem>
0010     <Operation type="Enumeration" value="Register"/>
0011     <RequestPayload>
0012         <ObjectType type="Enumeration" value="PrivateKey"/>
0013         <TemplateAttribute>
0014             <Attribute>
0015                 <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0016                 <AttributeValue type="Integer" value="Sign"/>
0017             </Attribute>
0018             <Attribute>
0019                 <AttributeName type="TextString" value="x-ID"/>
0020                 <AttributeValue type="TextString" value="TC-131-11-
prikey1"/>
0021             </Attribute>
0022         </TemplateAttribute>
0023         <PrivateKey>
0024             <KeyBlock>
0025                 <KeyFormatType type="Enumeration" value="PKCS_1"/>
0026                 <KeyValue>
0027                     <KeyMaterial type="ByteString"
value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353
57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483
46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa
2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650
89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c
795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f
91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281
5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050
203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a
7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f
a74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b
2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0
e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a
a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e
3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78
965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8
c3cdc2464744a793713dafb9f1dbc799ff96423fecdc3ba794286bce920f4b5c183f
99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967
4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c
ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064
b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e
59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4
990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766
b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab
7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0
e94ad1ee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db
e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa
e1ebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2
7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eaeaf922fd75d5b16b1a5
61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a72
```


0028	6a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d349417e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f8129c32341a8b44f"/>
0029	</KeyValue>
0030	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0031	<CryptographicLength type="Integer" value="2048"/>
0032	</KeyBlock>
0033	</PrivateKey>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="1"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Register"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0051	</ResponsePayload>
0052	</BatchItem>
0053	</ResponseMessage>
0054	# TIME 1
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="1"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="Register"/>
0065	<RequestPayload>
0066	<ObjectType type="Enumeration" value="PublicKey"/>
0067	<TemplateAttribute>
0068	<Attribute>
0069	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0070	<AttributeValue type="Integer" value="Verify"/>
0071	</Attribute>
0072	<Attribute>
0073	<AttributeName type="TextString" value="Link"/>
0074	<AttributeValue>
	<LinkType type="Enumeration" value="PrivateKeyLink"/>
	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>

0075	</AttributeValue>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-131-11- pubkey1"/>
0080	</Attribute>
0081	</TemplateAttribute>
0082	<PublicKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString" value="3082010a0282010100ab7f161c0042496ccd6c6d4dad9199734353577760 03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b 8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89 b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981 35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328 abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013 da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612 a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010 001"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0089	<CryptographicLength type="Integer" value="2048"/>
0090	</KeyBlock>
0091	</PublicKey>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="1"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0109	</ResponsePayload>
0110	</BatchItem>
0111	</ResponseMessage>
0112	# TIME 2 <RequestMessage>
0113	<RequestHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="1"/>
0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>

0120	<BatchItem>
0121	<Operation type="Enumeration" value="AddAttribute"/>
0122	<RequestPayload>
0123	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Link"/>
0126	<AttributeValue>
0127	<LinkType type="Enumeration" value="PublicKeyLink"/>
0128	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0129	</AttributeValue>
0130	</Attribute>
0131	</RequestPayload>
0132	</BatchItem>
0133	</RequestMessage>
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="1"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="AddAttribute"/>
0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0148	<Attribute>
0149	<AttributeName type="TextString" value="Link"/>
0150	<AttributeValue>
0151	<LinkType type="Enumeration" value="PublicKeyLink"/>
0152	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0153	</AttributeValue>
0154	</Attribute>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
	# TIME 3
0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="1"/>
0163	</ProtocolVersion>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Locate"/>
0168	<RequestPayload>
0169	<Attribute>
0170	<AttributeName type="TextString" value="Object Type"/>
0171	<AttributeValue type="Enumeration" value="PublicKey"/>

0172	</Attribute>
0173	<Attribute>
0174	<AttributeName type="TextString" value="Link"/>
0175	<AttributeValue>
0176	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0177	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0178	</AttributeValue>
0179	</Attribute>
0180	</RequestPayload>
0181	</BatchItem>
0182	</RequestMessage>
0183	<ResponseMessage>
0184	<ResponseHeader>
0185	<ProtocolVersion>
0186	<ProtocolVersionMajor type="Integer" value="1"/>
0187	<ProtocolVersionMinor type="Integer" value="1"/>
0188	</ProtocolVersion>
0189	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0190	<BatchCount type="Integer" value="1"/>
0191	</ResponseHeader>
0192	<BatchItem>
0193	<Operation type="Enumeration" value="Locate"/>
0194	<ResultStatus type="Enumeration" value="Success"/>
0195	<ResponsePayload>
0196	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0197	</ResponsePayload>
0198	</BatchItem>
0199	</ResponseMessage>
	# TIME 4
0200	<RequestMessage>
0201	<RequestHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="1"/>
0205	</ProtocolVersion>
0206	<BatchCount type="Integer" value="1"/>
0207	</RequestHeader>
0208	<BatchItem>
0209	<Operation type="Enumeration" value="Locate"/>
0210	<RequestPayload>
0211	<Attribute>
0212	<AttributeName type="TextString" value="Object Type"/>
0213	<AttributeValue type="Enumeration" value="PrivateKey"/>
0214	</Attribute>
0215	<Attribute>
0216	<AttributeName type="TextString" value="Link"/>
0217	<AttributeValue>
0218	<LinkType type="Enumeration" value="PublicKeyLink"/>
0219	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0220	</AttributeValue>
0221	</Attribute>
0222	</RequestPayload>
0223	</BatchItem>
0224	</RequestMessage>

0225	<ResponseMessage>
0226	<ResponseHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="1"/>
0230	</ProtocolVersion>
0231	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0232	<BatchCount type="Integer" value="1"/>
0233	</ResponseHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="Locate"/>
0236	<ResultStatus type="Enumeration" value="Success"/>
0237	<ResponsePayload>
0238	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0239	</ResponsePayload>
0240	</BatchItem>
0241	</ResponseMessage>
# TIME 5	
0242	<RequestMessage>
0243	<RequestHeader>
0244	<ProtocolVersion>
0245	<ProtocolVersionMajor type="Integer" value="1"/>
0246	<ProtocolVersionMinor type="Integer" value="1"/>
0247	</ProtocolVersion>
0248	<BatchCount type="Integer" value="1"/>
0249	</RequestHeader>
0250	<BatchItem>
0251	<Operation type="Enumeration" value="Get"/>
0252	<RequestPayload>
0253	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0254	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0255	</RequestPayload>
0256	</BatchItem>
0257	</RequestMessage>
0258	<ResponseMessage>
0259	<ResponseHeader>
0260	<ProtocolVersion>
0261	<ProtocolVersionMajor type="Integer" value="1"/>
0262	<ProtocolVersionMinor type="Integer" value="1"/>
0263	</ProtocolVersion>
0264	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0265	<BatchCount type="Integer" value="1"/>
0266	</ResponseHeader>
0267	<BatchItem>
0268	<Operation type="Enumeration" value="Get"/>
0269	<ResultStatus type="Enumeration" value="Success"/>
0270	<ResponsePayload>
0271	<ObjectType type="Enumeration" value="PrivateKey"/>
0272	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0273	<PrivateKey>
0274	<KeyBlock>
0275	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0276	<KeyValue>
0277	<KeyMaterial type="ByteString"

	<pre> value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353 57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483 46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa 2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650 89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c 795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f 91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281 5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050 203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a 7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f a74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b 2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0 e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e 3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78 965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8 c3cdc2464744a793713dafb9f1dbc799ff96423fecdc3ba794286bce920f4b5c183f 99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967 4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064 b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e 59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4 990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766 b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab 7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0 e94adlee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa elebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2 7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eae9a922fd75d5b16b1a5 61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a72 6ald90260e4f1084f518234dcd3fe770b952015bd543bb6a4117718754676a34171 666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520 a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a 1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d34941 7e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f812 9c32341a8b44f"/> </pre>
0278	</KeyValue>
0279	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0280	<CryptographicLength type="Integer" value="2048"/>
0281	</KeyBlock>
0282	</PrivateKey>
0283	</ResponsePayload>
0284	</BatchItem>
0285	</ResponseMessage>
	# TIME 6
0286	<RequestMessage>
0287	<RequestHeader>
0288	<ProtocolVersion>
0289	<ProtocolVersionMajor type="Integer" value="1"/>
0290	<ProtocolVersionMinor type="Integer" value="1"/>
0291	</ProtocolVersion>
0292	<BatchCount type="Integer" value="1"/>
0293	</RequestHeader>
0294	<BatchItem>
0295	<Operation type="Enumeration" value="Get"/>
0296	<RequestPayload>
0297	<UniqueIdentifier type="TextString"

0298	value="\$UNIQUE_IDENTIFIER_1"/>
0299	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0300	</RequestPayload>
0301	</BatchItem>
0302	</RequestMessage>
0302	<ResponseMessage>
0303	<ResponseHeader>
0304	<ProtocolVersion>
0305	<ProtocolVersionMajor type="Integer" value="1"/>
0306	<ProtocolVersionMinor type="Integer" value="1"/>
0307	</ProtocolVersion>
0308	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0309	<BatchCount type="Integer" value="1"/>
0310	</ResponseHeader>
0311	<BatchItem>
0312	<Operation type="Enumeration" value="Get"/>
0313	<ResultStatus type="Enumeration" value="Success"/>
0314	<ResponsePayload>
0315	<ObjectType type="Enumeration" value="PublicKey"/>
0316	<UniqueIdentifier type="TextString"
0317	value="\$UNIQUE_IDENTIFIER_1"/>
0318	<PublicKey>
0319	<KeyBlock>
0320	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0321	<KeyValue>
0322	<KeyMaterial type="ByteString"
0323	value="3082010a0282010100ab7f161c0042496ccd6c6d4dad9199734353577760
0324	03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b
0325	8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89
0326	b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981
0327	35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328
0328	abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013
0329	da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612
0330	a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010
0331	001"/>
0332	</KeyValue>
0333	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0334	<CryptographicLength type="Integer" value="2048"/>
0335	</KeyBlock>
0336	</PublicKey>
0337	</ResponsePayload>
0338	</BatchItem>
0339	</ResponseMessage>
0330	# TIME 7
0331	<RequestMessage>
0332	<RequestHeader>
0333	<ProtocolVersion>
0334	<ProtocolVersionMajor type="Integer" value="1"/>
0335	<ProtocolVersionMinor type="Integer" value="1"/>
0336	</ProtocolVersion>
0337	<BatchCount type="Integer" value="1"/>
0338	</RequestHeader>
0339	<BatchItem>
0340	<Operation type="Enumeration" value="Destroy"/>
0341	<RequestPayload>
0342	<UniqueIdentifier type="TextString"
0343	value="\$UNIQUE_IDENTIFIER_0"/>

0342	</RequestPayload>
0343	</BatchItem>
0344	</RequestMessage>
0345	<ResponseMessage>
0346	<ResponseHeader>
0347	<ProtocolVersion>
0348	<ProtocolVersionMajor type="Integer" value="1"/>
0349	<ProtocolVersionMinor type="Integer" value="1"/>
0350	</ProtocolVersion>
0351	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0352	<BatchCount type="Integer" value="1"/>
0353	</ResponseHeader>
0354	<BatchItem>
0355	<Operation type="Enumeration" value="Destroy"/>
0356	<ResultStatus type="Enumeration" value="Success"/>
0357	<ResponsePayload>
0358	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0359	</ResponsePayload>
0360	</BatchItem>
0361	</ResponseMessage>
	# TIME 8
0362	<RequestMessage>
0363	<RequestHeader>
0364	<ProtocolVersion>
0365	<ProtocolVersionMajor type="Integer" value="1"/>
0366	<ProtocolVersionMinor type="Integer" value="1"/>
0367	</ProtocolVersion>
0368	<BatchCount type="Integer" value="1"/>
0369	</RequestHeader>
0370	<BatchItem>
0371	<Operation type="Enumeration" value="Destroy"/>
0372	<RequestPayload>
0373	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0374	</RequestPayload>
0375	</BatchItem>
0376	</RequestMessage>
0377	<ResponseMessage>
0378	<ResponseHeader>
0379	<ProtocolVersion>
0380	<ProtocolVersionMajor type="Integer" value="1"/>
0381	<ProtocolVersionMinor type="Integer" value="1"/>
0382	</ProtocolVersion>
0383	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0384	<BatchCount type="Integer" value="1"/>
0385	</ResponseHeader>
0386	<BatchItem>
0387	<Operation type="Enumeration" value="Destroy"/>
0388	<ResultStatus type="Enumeration" value="Success"/>
0389	<ResponsePayload>
0390	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0391	</ResponsePayload>
0392	</BatchItem>
0393	</ResponseMessage>

515

516 2.2.25 TC-132-11 - Register an Asymmetric Key Pair and a Corresponding
517 X509 Certificate

518 Register a public/private key pair in the PKCS_1 key format and a corresponding X509 certificate.
519 Add the appropriate links between the registered objects. Make sure the certificate was
520 registered and the attributes set correctly by listing and retrieving the attributes. Get the keys
521 and certificate, and finally destroy all the registered objects.

```
# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="1"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="Register"/>
0011     <RequestPayload>
0012       <ObjectType type="Enumeration" value="PublicKey"/>
0013       <TemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0016           <AttributeValue type="Integer" value="Verify"/>
0017         </Attribute>
0018         <Attribute>
0019           <AttributeName type="TextString" value="x-ID"/>
0020           <AttributeValue type="TextString" value="TC-132-11-
pubkey1"/>
0021         </Attribute>
0022       </TemplateAttribute>
0023       <PublicKey>
0024         <KeyBlock>
0025           <KeyFormatType type="Enumeration" value="PKCS_1"/>
0026           <KeyValue>
0027             <KeyMaterial type="ByteString"
value="3082010a0282010100ab7f161c0042496ccd6c6d4dadb9199734353577760
03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b
8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89
b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981
35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328
abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013
da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612
a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010
001"/>
0028           </KeyValue>
0029           <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0030           <CryptographicLength type="Integer" value="2048"/>
0031         </KeyBlock>
0032       </PublicKey>
0033     </RequestPayload>
```

0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="1"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="1"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PrivateKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0068	<AttributeValue type="Integer" value="Sign"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>
0073	<LinkType type="Enumeration" value="PublicKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0075	</AttributeValue>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-132-11-
	prikey1"/>
0080	</Attribute>
0081	</TemplateAttribute>
0082	<PrivateKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0085	<KeyValue>

0086	<pre> <KeyMaterial type="ByteString" value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353 57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483 46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa 2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650 89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c 795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f 91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281 5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050 203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a 7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f a74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b 2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0 e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e 3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78 965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8 c3cdc2464744a793713dafb9f1dbc799ff96423fecdc3ba794286bce920f4b5c183f 99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967 4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064 b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e 59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4 990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766 b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab 7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0 e94adlee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa elebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2 7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eaeafa922fd75d5b16b1a5 61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a72 6a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171 666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520 a2cea35800ad2724led360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a 1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d34941 7e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f812 9c32341a8b44f"/> </pre>
0087	<pre></KeyValue></pre>
0088	<pre><CryptographicAlgorithm type="Enumeration" value="RSA"/></pre>
0089	<pre><CryptographicLength type="Integer" value="2048"/></pre>
0090	<pre></KeyBlock></pre>
0091	<pre></PrivateKey></pre>
0092	<pre></RequestPayload></pre>
0093	<pre></BatchItem></pre>
0094	<pre></RequestMessage></pre>
0095	<pre><ResponseMessage></pre>
0096	<pre><ResponseHeader></pre>
0097	<pre><ProtocolVersion></pre>
0098	<pre><ProtocolVersionMajor type="Integer" value="1"/></pre>
0099	<pre><ProtocolVersionMinor type="Integer" value="1"/></pre>
0100	<pre></ProtocolVersion></pre>
0101	<pre><TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/></pre>
0102	<pre><BatchCount type="Integer" value="1"/></pre>
0103	<pre></ResponseHeader></pre>
0104	<pre><BatchItem></pre>
0105	<pre><Operation type="Enumeration" value="Register"/></pre>
0106	<pre><ResultStatus type="Enumeration" value="Success"/></pre>

0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString"
0109	value="\$UNIQUE_IDENTIFIER_1"/>
0110	</ResponsePayload>
0111	</BatchItem>
0111	</ResponseMessage>
# TIME 2	
0112	<RequestMessage>
0113	<RequestHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="1"/>
0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="Register"/>
0122	<RequestPayload>
0123	<ObjectType type="Enumeration" value="Certificate"/>
0124	<TemplateAttribute>
0125	<Attribute>
0126	<AttributeName type="TextString" value="Cryptographic
0127	Usage Mask"/>
0128	<AttributeValue type="Integer" value="Verify Sign"/>
0129	</Attribute>
0130	<Attribute>
0131	<AttributeName type="TextString" value="Link"/>
0132	<AttributeValue>
0133	<LinkType type="Enumeration" value="PublicKeyLink"/>
0134	<LinkedObjectIdentifier type="TextString"
0135	value="\$UNIQUE_IDENTIFIER_0"/>
0136	</Attribute>
0137	<Attribute>
0138	<AttributeName type="TextString" value="x-ID"/>
0139	<AttributeValue type="TextString" value="TC-132-11-
0140	cert1"/>
0141	</Attribute>
0142	</TemplateAttribute>
0143	<Certificate>
0144	<CertificateType type="Enumeration" value="X_509"/>
0145	<CertificateValue type="ByteString"
0146	value="30820312308201faa003020102020101300d06092a864886f70d010105050
0147	0303b310b3009060355040613025553310d300b060355040a130454455354310e300
0148	c060355040b13054f41534953310d300b060355040313044b4d4950301e170d31303
0149	13130313233353935395a170d3230313130313233353935395a303b310b300906035
0150	5040613025553310d300b060355040a130454455354310e300c060355040b13054f4
0151	1534953310d300b060355040313044b4d495030820122300d06092a864886f70d010
0152	10105000382010f003082010a0282010100ab7f161c0042496ccd6c6d4dadb919973
0153	435357776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74
0154	648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc62
0155	67fa2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8
0156	b65089f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295
0157	353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142c
0158	b76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1
0159	c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f
0160	6050203010001a321301f301d0603551d0e0416041404e57bd2c431b2e816e180a19

0144	823fac858273f6b300d06092a864886f70d01010505000382010100a876adbc6c8e0 ff017216e195fea76bfff61a567c9a13dc50d13fec12a4273c441547cfabcb5d61d99 1e966319df72c0d41ba826a45112ff26089a2344f4d71cf7c921b4bdfaef1600d1ba aa15336057e014b8b496d4fae9e8a6c1da9aeb6cbc960cbf2fae77f587ec4bb28204 5338845b88dd9aeea53e482a36e734e4f5f03b9d0dfc4cafc6bb34ea9053e52bd609 ee01e86d9b09fb51120c19834a997b09ce08d79e81311762f974bb1c8c09186c4d78 933e0db38e905084877e147c78af52fae07192ff166d19fa94a11cc11b27ed050f7a 27fae13b205a574c4ee00aa8bd65d0d7057c985c839ef336a441ed53a53c6b6b696f 1bdeb5f7ea811ebb25a7f86"/>
0145	</Certificate>
0146	</RequestPayload>
0147	</BatchItem>
0148	</RequestMessage>
0148	<ResponseMessage>
0149	<ResponseHeader>
0150	<ProtocolVersion>
0151	<ProtocolVersionMajor type="Integer" value="1"/>
0152	<ProtocolVersionMinor type="Integer" value="1"/>
0153	</ProtocolVersion>
0154	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0155	<BatchCount type="Integer" value="1"/>
0156	</ResponseHeader>
0157	<BatchItem>
0158	<Operation type="Enumeration" value="Register"/>
0159	<ResultStatus type="Enumeration" value="Success"/>
0160	<ResponsePayload>
0161	<UniqueIdentifier type="TextString"
0162	value="\$UNIQUE_IDENTIFIER_2"/>
0163	</ResponsePayload>
0164	</BatchItem>
0165	</ResponseMessage>
0165	# TIME 3
0166	<RequestMessage>
0167	<RequestHeader>
0168	<ProtocolVersion>
0169	<ProtocolVersionMajor type="Integer" value="1"/>
0170	<ProtocolVersionMinor type="Integer" value="1"/>
0171	</ProtocolVersion>
0172	<BatchCount type="Integer" value="2"/>
0173	</RequestHeader>
0174	<BatchItem>
0175	<Operation type="Enumeration" value="AddAttribute"/>
0176	<UniqueBatchItemID type="ByteString" value="31f81bfb0f0492bd"/>
0177	<RequestPayload>
0178	<UniqueIdentifier type="TextString"
0179	value="\$UNIQUE_IDENTIFIER_0"/>
0180	<Attribute>
0181	<AttributeName type="TextString" value="Link"/>
0182	<AttributeValue>
0183	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0184	<LinkedObjectIdentifier type="TextString"
0185	value="\$UNIQUE_IDENTIFIER_1"/>
0186	</AttributeValue>
0187	</Attribute>
0188	</RequestPayload>
0189	</BatchItem>
0190	</BatchItem>

0188	<Operation type="Enumeration" value="AddAttribute"/>
0189	<UniqueBatchItemID type="ByteString" value="ba865701c7837be2"/>
0190	<RequestPayload>
0191	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0192	<Attribute>
0193	<AttributeName type="TextString" value="Link"/>
0194	<AttributeValue>
0195	<LinkType type="Enumeration" value="CertificateLink"/>
0196	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0197	</AttributeValue>
0198	</Attribute>
0199	</RequestPayload>
0200	</BatchItem>
0201	</RequestMessage>
0202	<ResponseMessage>
0203	<ResponseHeader>
0204	<ProtocolVersion>
0205	<ProtocolVersionMajor type="Integer" value="1"/>
0206	<ProtocolVersionMinor type="Integer" value="1"/>
0207	</ProtocolVersion>
0208	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0209	<BatchCount type="Integer" value="2"/>
0210	</ResponseHeader>
0211	<BatchItem>
0212	<Operation type="Enumeration" value="AddAttribute"/>
0213	<UniqueBatchItemID type="ByteString" value="31f81bfb0f0492bd"/>
0214	<ResultStatus type="Enumeration" value="Success"/>
0215	<ResponsePayload>
0216	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0217	<Attribute>
0218	<AttributeName type="TextString" value="Link"/>
0219	<AttributeValue>
0220	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0221	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0222	</AttributeValue>
0223	</Attribute>
0224	</ResponsePayload>
0225	</BatchItem>
0226	<BatchItem>
0227	<Operation type="Enumeration" value="AddAttribute"/>
0228	<UniqueBatchItemID type="ByteString" value="ba865701c7837be2"/>
0229	<ResultStatus type="Enumeration" value="Success"/>
0230	<ResponsePayload>
0231	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0232	<Attribute>
0233	<AttributeName type="TextString" value="Link"/>
0234	<AttributeIndex type="Integer" value="1"/>
0235	<AttributeValue>
0236	<LinkType type="Enumeration" value="CertificateLink"/>
0237	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0238	</AttributeValue>

0239	</Attribute>
0240	</ResponsePayload>
0241	</BatchItem>
0242	</ResponseMessage>
# TIME 4	
0243	<RequestMessage>
0244	<RequestHeader>
0245	<ProtocolVersion>
0246	<ProtocolVersionMajor type="Integer" value="1"/>
0247	<ProtocolVersionMinor type="Integer" value="1"/>
0248	</ProtocolVersion>
0249	<BatchCount type="Integer" value="1"/>
0250	</RequestHeader>
0251	<BatchItem>
0252	<Operation type="Enumeration" value="GetAttributeList"/>
0253	<RequestPayload>
0254	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0255	</RequestPayload>
0256	</BatchItem>
0257	</RequestMessage>
0258	<ResponseMessage>
0259	<ResponseHeader>
0260	<ProtocolVersion>
0261	<ProtocolVersionMajor type="Integer" value="1"/>
0262	<ProtocolVersionMinor type="Integer" value="1"/>
0263	</ProtocolVersion>
0264	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0265	<BatchCount type="Integer" value="1"/>
0266	</ResponseHeader>
0267	<BatchItem>
0268	<Operation type="Enumeration" value="GetAttributeList"/>
0269	<ResultStatus type="Enumeration" value="Success"/>
0270	<ResponsePayload>
0271	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0272	<AttributeName type="TextString" value="Cryptographic Length"/>
0273	<AttributeName type="TextString" value="Certificate Length"/>
0274	<AttributeName type="TextString" value="X.509 Certificate Identifier"/>
0275	<AttributeName type="TextString" value="X.509 Certificate Issuer"/>
0276	<AttributeName type="TextString" value="X.509 Certificate Subject"/>
0277	<AttributeName type="TextString" value="Digital Signature Algorithm"/>
0278	<AttributeName type="TextString" value="Fresh"/>
0279	<AttributeName type="TextString" value="Certificate Issuer"/>
0280	<AttributeName type="TextString" value="Certificate Type"/>
0281	<AttributeName type="TextString" value="Certificate Subject"/>
0282	<AttributeName type="TextString" value="Certificate Identifier"/>
0283	<AttributeName type="TextString" value="State"/>
0284	<AttributeName type="TextString" value="Digest"/>
0285	<AttributeName type="TextString" value="Link"/>
0286	<AttributeName type="TextString" value="Lease Time"/>

0287	<AttributeName type="TextString" value="Initial Date"/>
0288	<AttributeName type="TextString" value="Unique Identifier"/>
0289	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0290	<AttributeName type="TextString" value="Object Type"/>
0291	<AttributeName type="TextString" value="Last Change Date"/>
0292	<AttributeName type="TextString" value="x-ID"/>
0293	</ResponsePayload>
0294	</BatchItem>
0295	</ResponseMessage>
# TIME 5	
0296	<RequestMessage>
0297	<RequestHeader>
0298	<ProtocolVersion>
0299	<ProtocolVersionMajor type="Integer" value="1"/>
0300	<ProtocolVersionMinor type="Integer" value="1"/>
0301	</ProtocolVersion>
0302	<BatchCount type="Integer" value="1"/>
0303	</RequestHeader>
0304	<BatchItem>
0305	<Operation type="Enumeration" value="GetAttributes"/>
0306	<RequestPayload>
0307	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0308	<AttributeName type="TextString" value="Certificate Identifier"/>
0309	<AttributeName type="TextString" value="Certificate Issuer"/>
0310	<AttributeName type="TextString" value="Certificate Subject"/>
0311	<AttributeName type="TextString" value="Certificate Type"/>
0312	<AttributeName type="TextString" value="Digital Signature Algorithm"/>
0313	<AttributeName type="TextString" value="Cryptographic Length"/>
0314	</RequestPayload>
0315	</BatchItem>
0316	</RequestMessage>
0317	<ResponseMessage>
0318	<ResponseHeader>
0319	<ProtocolVersion>
0320	<ProtocolVersionMajor type="Integer" value="1"/>
0321	<ProtocolVersionMinor type="Integer" value="1"/>
0322	</ProtocolVersion>
0323	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0324	<BatchCount type="Integer" value="1"/>
0325	</ResponseHeader>
0326	<BatchItem>
0327	<Operation type="Enumeration" value="GetAttributes"/>
0328	<ResultStatus type="Enumeration" value="Success"/>
0329	<ResponsePayload>
0330	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0331	<Attribute>
0332	<AttributeName type="TextString" value="Certificate Identifier"/>
0333	<AttributeValue>
0334	<Issuer type="TextString" value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>

0335	<SerialNumber type="TextString" value="1"/>
0336	</AttributeValue>
0337	</Attribute>
0338	<Attribute>
0339	<AttributeName type="TextString" value="Certificate Issuer"/>
0340	<AttributeValue>
0341	<CertificateIssuerDistinguishedName type="TextString" value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0342	</AttributeValue>
0343	</Attribute>
0344	<Attribute>
0345	<AttributeName type="TextString" value="Certificate Subject"/>
0346	<AttributeValue>
0347	<CertificateSubjectDistinguishedName type="TextString" value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0348	</AttributeValue>
0349	</Attribute>
0350	<Attribute>
0351	<AttributeName type="TextString" value="Certificate Type"/>
0352	<AttributeValue type="Enumeration" value="X_509"/>
0353	</Attribute>
0354	<Attribute>
0355	<AttributeName type="TextString" value="Digital Signature Algorithm"/>
0356	<AttributeValue type="Enumeration" value="SHA_1WithRSAEncryption"/>
0357	</Attribute>
0358	<Attribute>
0359	<AttributeName type="TextString" value="Cryptographic Length"/>
0360	<AttributeValue type="Integer" value="2048"/>
0361	</Attribute>
0362	</ResponsePayload>
0363	</BatchItem>
0364	</ResponseMessage>
# TIME 6	
0365	<RequestMessage>
0366	<RequestHeader>
0367	<ProtocolVersion>
0368	<ProtocolVersionMajor type="Integer" value="1"/>
0369	<ProtocolVersionMinor type="Integer" value="1"/>
0370	</ProtocolVersion>
0371	<BatchCount type="Integer" value="1"/>
0372	</RequestHeader>
0373	<BatchItem>
0374	<Operation type="Enumeration" value="Get"/>
0375	<RequestPayload>
0376	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0377	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0378	</RequestPayload>
0379	</BatchItem>
0380	</RequestMessage>
0381	<ResponseMessage>
0382	<ResponseHeader>

```
0383     <ProtocolVersion>
0384         <ProtocolVersionMajor type="Integer" value="1"/>
0385         <ProtocolVersionMinor type="Integer" value="1"/>
0386     </ProtocolVersion>
0387     <TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0388     <BatchCount type="Integer" value="1"/>
0389 </ResponseHeader>
0390 <BatchItem>
0391     <Operation type="Enumeration" value="Get"/>
0392     <ResultStatus type="Enumeration" value="Success"/>
0393     <ResponsePayload>
0394         <ObjectType type="Enumeration" value="PrivateKey"/>
0395         <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0396         <PrivateKey>
0397             <KeyBlock>
0398                 <KeyFormatType type="Enumeration" value="PKCS_1"/>
0399                 <KeyValue>
0400                     <KeyMaterial type="ByteString"
value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353
57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483
46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa
2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650
89f98135b1c67b701675abdb7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c
795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f
91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281
5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050
203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a
7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f
a74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b
2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0
e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a
a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e
3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78
965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8
c3cdc2464744a793713dafb9f1dbc799ff96423fecdc3ba794286bce920f4b5c183f
99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967
4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c
ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064
b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e
59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4
990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766
b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab
7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0
e94ad1ee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db
e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa
e1ebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2
7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eae922fd75d5b16b1a5
61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a72
6a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171
666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520
a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a
1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d34941
7e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f812
9c32341a8b44f"/>
0401             </KeyValue>
0402         <CryptographicAlgorithm type="Enumeration" value="RSA"/>
```

0403	<CryptographicLength type="Integer" value="2048"/>
0404	</KeyBlock>
0405	</PrivateKey>
0406	</ResponsePayload>
0407	</BatchItem>
0408	</ResponseMessage>
# TIME 7	
0409	<RequestMessage>
0410	<RequestHeader>
0411	<ProtocolVersion>
0412	<ProtocolVersionMajor type="Integer" value="1"/>
0413	<ProtocolVersionMinor type="Integer" value="1"/>
0414	</ProtocolVersion>
0415	<BatchCount type="Integer" value="1"/>
0416	</RequestHeader>
0417	<BatchItem>
0418	<Operation type="Enumeration" value="Get"/>
0419	<RequestPayload>
0420	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0421	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0422	</RequestPayload>
0423	</BatchItem>
0424	</RequestMessage>
0425	<ResponseMessage>
0426	<ResponseHeader>
0427	<ProtocolVersion>
0428	<ProtocolVersionMajor type="Integer" value="1"/>
0429	<ProtocolVersionMinor type="Integer" value="1"/>
0430	</ProtocolVersion>
0431	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0432	<BatchCount type="Integer" value="1"/>
0433	</ResponseHeader>
0434	<BatchItem>
0435	<Operation type="Enumeration" value="Get"/>
0436	<ResultStatus type="Enumeration" value="Success"/>
0437	<ResponsePayload>
0438	<ObjectType type="Enumeration" value="PublicKey"/>
0439	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0440	<PublicKey>
0441	<KeyBlock>
0442	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0443	<KeyValue>
0444	<KeyMaterial type="ByteString" value="3082010a0282010100ab7f161c0042496ccd6c6d4dadb9199734353577760 03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b 8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89 b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981 35b1c67b701675abdbc7d5721aac9d14a7f081fcce80b64e8a0ecc8295353c795328 abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013 da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612 a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010 001"/>
0445	</KeyValue>
0446	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0447	<CryptographicLength type="Integer" value="2048"/>

0448	</KeyBlock>
0449	</PublicKey>
0450	</ResponsePayload>
0451	</BatchItem>
0452	</ResponseMessage>
0453	# TIME 8 <RequestMessage>
0454	<RequestHeader>
0455	<ProtocolVersion>
0456	<ProtocolVersionMajor type="Integer" value="1"/>
0457	<ProtocolVersionMinor type="Integer" value="1"/>
0458	</ProtocolVersion>
0459	<BatchCount type="Integer" value="1"/>
0460	</RequestHeader>
0461	<BatchItem>
0462	<Operation type="Enumeration" value="Get"/>
0463	<RequestPayload>
0464	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0465	</RequestPayload>
0466	</BatchItem>
0467	</RequestMessage>
0468	<ResponseMessage>
0469	<ResponseHeader>
0470	<ProtocolVersion>
0471	<ProtocolVersionMajor type="Integer" value="1"/>
0472	<ProtocolVersionMinor type="Integer" value="1"/>
0473	</ProtocolVersion>
0474	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0475	<BatchCount type="Integer" value="1"/>
0476	</ResponseHeader>
0477	<BatchItem>
0478	<Operation type="Enumeration" value="Get"/>
0479	<ResultStatus type="Enumeration" value="Success"/>
0480	<ResponsePayload>
0481	<ObjectType type="Enumeration" value="Certificate"/>
0482	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0483	<Certificate>
0484	<CertificateType type="Enumeration" value="X_509"/>
0485	<CertificateValue type="ByteString" value="30820312308201faa003020102020101300d06092a864886f70d010105050 0303b310b3009060355040613025553310d300b060355040a130454455354310e300 c060355040b13054f41534953310d300b060355040313044b4d4950301e170d31303 13130313233353935395a170d3230313130313233353935395a303b310b300906035 5040613025553310d300b060355040a130454455354310e300c060355040b13054f4 1534953310d300b060355040313044b4d495030820122300d06092a864886f70d010 10105000382010f003082010a0282010100ab7f161c0042496ccd6c6d4dad919973 435357776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74 648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc62 67fa2a6f89b9bee9e60ald7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8 b65089f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295 353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142c b76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1 c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f 6050203010001a321301f301d0603551d0e0416041404e57bd2c431b2e816e180a19 823fac858273f6b300d06092a864886f70d01010505000382010100a876adbc6c8e0

0486	ff017216e195fea76bfff61a567c9a13dc50d13fec12a4273c441547cfabcb5d61d99
0487	1e966319df72c0d41ba826a45112ff26089a2344f4d71cf7c921b4bdfaef1600d1ba
0488	aa15336057e014b8b496d4fae9e8a6c1da9aeb6cbc960cbf2fae77f587ec4bb28204
0489	5338845b88dd9aeaa53e482a36e734e4f5f03b9d0dfc4cafc6bb34ea9053e52bd609
	ee01e86d9b09fb51120c19834a997b09ce08d79e81311762f974bb1c8c09186c4d78
	933e0db38e905084877e147c78af52fae07192ff166d19fa94a11cc11b27ed050f7a
	27fae13b205a574c4ee00aa8bd65d0d7057c985c839ef336a441ed53a53c6b6b696f
	1bdeb5f7ea811ebb25a7f86"/>
	</Certificate>
	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>
0490	# TIME 9
0491	<RequestMessage>
0492	<RequestHeader>
0493	<ProtocolVersion>
0494	<ProtocolVersionMajor type="Integer" value="1"/>
0495	<ProtocolVersionMinor type="Integer" value="1"/>
0496	</ProtocolVersion>
0497	<BatchCount type="Integer" value="1"/>
0498	</BatchCount>
0499	<Operation type="Enumeration" value="Destroy"/>
0500	<RequestPayload>
0501	<UniqueIdentifier type="TextString"
0502	value="\$UNIQUE_IDENTIFIER_1"/>
0503	</UniqueIdentifier>
0504	</RequestPayload>
0505	</BatchItem>
0506	</RequestMessage>
0507	<ResponseMessage>
0508	<ResponseHeader>
0509	<ProtocolVersion>
0510	<ProtocolVersionMajor type="Integer" value="1"/>
0511	<ProtocolVersionMinor type="Integer" value="1"/>
0512	</ProtocolVersion>
0513	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0514	<BatchCount type="Integer" value="1"/>
0515	</BatchCount>
0516	<Operation type="Enumeration" value="Destroy"/>
0517	<ResultStatus type="Enumeration" value="Success"/>
0518	<ResponsePayload>
0519	<UniqueIdentifier type="TextString"
0520	value="\$UNIQUE_IDENTIFIER_1"/>
0521	</UniqueIdentifier>
0522	</ResponsePayload>
0523	</BatchItem>
0524	</ResponseMessage>
0525	# TIME 10
0526	<RequestMessage>
0527	<RequestHeader>
0528	<ProtocolVersion>
0529	<ProtocolVersionMajor type="Integer" value="1"/>
	<ProtocolVersionMinor type="Integer" value="1"/>
	</ProtocolVersion>
	<BatchCount type="Integer" value="1"/>
	</BatchCount>
	</RequestHeader>

0530	<BatchItem>
0531	<Operation type="Enumeration" value="Destroy"/>
0532	<RequestPayload>
0533	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0534	</RequestPayload>
0535	</BatchItem>
0536	</RequestMessage>
0537	<ResponseMessage>
0538	<ResponseHeader>
0539	<ProtocolVersion>
0540	<ProtocolVersionMajor type="Integer" value="1"/>
0541	<ProtocolVersionMinor type="Integer" value="1"/>
0542	</ProtocolVersion>
0543	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0544	<BatchCount type="Integer" value="1"/>
0545	</ResponseHeader>
0546	<BatchItem>
0547	<Operation type="Enumeration" value="Destroy"/>
0548	<ResultStatus type="Enumeration" value="Success"/>
0549	<ResponsePayload>
0550	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0551	</ResponsePayload>
0552	</BatchItem>
0553	</ResponseMessage>
	# TIME 11
0554	<RequestMessage>
0555	<RequestHeader>
0556	<ProtocolVersion>
0557	<ProtocolVersionMajor type="Integer" value="1"/>
0558	<ProtocolVersionMinor type="Integer" value="1"/>
0559	</ProtocolVersion>
0560	<BatchCount type="Integer" value="1"/>
0561	</RequestHeader>
0562	<BatchItem>
0563	<Operation type="Enumeration" value="Destroy"/>
0564	<RequestPayload>
0565	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0566	</RequestPayload>
0567	</BatchItem>
0568	</RequestMessage>
0569	<ResponseMessage>
0570	<ResponseHeader>
0571	<ProtocolVersion>
0572	<ProtocolVersionMajor type="Integer" value="1"/>
0573	<ProtocolVersionMinor type="Integer" value="1"/>
0574	</ProtocolVersion>
0575	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0576	<BatchCount type="Integer" value="1"/>
0577	</ResponseHeader>
0578	<BatchItem>
0579	<Operation type="Enumeration" value="Destroy"/>
0580	<ResultStatus type="Enumeration" value="Success"/>
0581	<ResponsePayload>

0582	<code><UniqueIdentifier type="TextString"</code>
	<code>value="\$UNIQUE_IDENTIFIER_2"/></code>
0583	<code></ResponsePayload></code>
0584	<code></BatchItem></code>
0585	<code></ResponseMessage></code>

522

523 2.2.26 TC-133-11 - Create, Re-key Key Pair

524 Create a public/private key pair on the server and retrieve the keys in PKCS_1 format. Re-key the
525 key pair and retrieve the new public/private key pair in transparent format. To verify that the
526 links are set correctly, the Link attributes are retrieved. Finally, all the keys are destroyed.

527 Note: a server is not required to support conversion between key formats so returning keys in
528 Transparent form when registered in PKCS_1 may not be supported.

	<code># TIME 0</code>
0001	<code><RequestMessage></code>
0002	<code><RequestHeader></code>
0003	<code><ProtocolVersion></code>
0004	<code><ProtocolVersionMajor type="Integer" value="1"/></code>
0005	<code><ProtocolVersionMinor type="Integer" value="1"/></code>
0006	<code></ProtocolVersion></code>
0007	<code><BatchCount type="Integer" value="1"/></code>
0008	<code></RequestHeader></code>
0009	<code><BatchItem></code>
0010	<code><Operation type="Enumeration" value="CreateKeyPair"/></code>
0011	<code><RequestPayload></code>
0012	<code><CommonTemplateAttribute></code>
0013	<code><Attribute></code>
0014	<code><AttributeName type="TextString" value="Cryptographic</code>
	<code>Algorithm"/></code>
0015	<code><AttributeValue type="Enumeration" value="RSA"/></code>
0016	<code></Attribute></code>
0017	<code><Attribute></code>
0018	<code><AttributeName type="TextString" value="Cryptographic</code>
	<code>Length"/></code>
0019	<code><AttributeValue type="Integer" value="2048"/></code>
0020	<code></Attribute></code>
0021	<code></CommonTemplateAttribute></code>
0022	<code><PrivateKeyTemplateAttribute></code>
0023	<code><Attribute></code>
0024	<code><AttributeName type="TextString" value="Name"/></code>
0025	<code><AttributeValue></code>
0026	<code><NameValue type="TextString" value="TC-133-11-</code>
	<code>privateKey1"/></code>
0027	<code><NameType type="Enumeration"</code>
	<code>value="UninterpretedTextString"/></code>
0028	<code></AttributeValue></code>
0029	<code></Attribute></code>
0030	<code><Attribute></code>
0031	<code><AttributeName type="TextString" value="Cryptographic</code>
	<code>Usage Mask"/></code>
0032	<code><AttributeValue type="Integer" value="Sign"/></code>
0033	<code></Attribute></code>

0034	</PrivateKeyTemplateAttribute>
0035	<PublicKeyTemplateAttribute>
0036	<Attribute>
0037	<AttributeName type="TextString" value="Name"/>
0038	<AttributeValue>
0039	<NameValue type="TextString" value="TC-133-11- publicKey1"/>
0040	<NameType type="Enumeration" value="UninterpretedTextString"/>
0041	</AttributeValue>
0042	</Attribute>
0043	<Attribute>
0044	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0045	<AttributeValue type="Integer" value="Verify"/>
0046	</Attribute>
0047	</PublicKeyTemplateAttribute>
0048	</RequestPayload>
0049	</BatchItem>
0050	</RequestMessage>
0051	<ResponseMessage>
0052	<ResponseHeader>
0053	<ProtocolVersion>
0054	<ProtocolVersionMajor type="Integer" value="1"/>
0055	<ProtocolVersionMinor type="Integer" value="1"/>
0056	</ProtocolVersion>
0057	<TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/>
0058	<BatchCount type="Integer" value="1"/>
0059	</ResponseHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="CreateKeyPair"/>
0062	<ResultStatus type="Enumeration" value="Success"/>
0063	<ResponsePayload>
0064	<PrivateKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0065	<PublicKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
	# TIME 1
0069	<RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="1"/>
0074	</ProtocolVersion>
0075	<BatchCount type="Integer" value="1"/>
0076	</RequestHeader>
0077	<BatchItem>
0078	<Operation type="Enumeration" value="Get"/>
0079	<RequestPayload>
0080	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0081	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0082	</RequestPayload>
0083	</BatchItem>

0084	</RequestMessage>
0085	<ResponseMessage>
0086	<ResponseHeader>
0087	<ProtocolVersion>
0088	<ProtocolVersionMajor type="Integer" value="1"/>
0089	<ProtocolVersionMinor type="Integer" value="1"/>
0090	</ProtocolVersion>
0091	<TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/>
0092	<BatchCount type="Integer" value="1"/>
0093	</ResponseHeader>
0094	<BatchItem>
0095	<Operation type="Enumeration" value="Get"/>
0096	<ResultStatus type="Enumeration" value="Success"/>
0097	<ResponsePayload>
0098	<ObjectType type="Enumeration" value="PrivateKey"/>
0099	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0100	<PrivateKey>
0101	<KeyBlock>
0102	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0103	<KeyValue>
0104	<KeyMaterial type="ByteString"
	value="308204a30201000282010100b0612bccafdd11d41819a274526d68dbf3c3f 25667c402a0e0e8e4cce007ea6b6ea53699e8bd7ccab7d5ae66c00b28fd678b81ba1 d4e841c3a36caf13f852004633f80d840be7aad9bcdeabde11514b6ab3bce602e113 05cf5e9c34abee32c3c468b9b146502738c0ae82e63ab8bd1fc4db0c6a09eb0c9f6e 01b9cc8d22317aedab328209a1dc5d2ce8529d81521c41730c1c8c76249d233e8909 6ca44dfefb469e3532bb90d6691c6932d0c63dbb7647c6e64337b719a1f100b1366cf f3bbb213b17c716beb2c9ad88b3b76abacc378c4898636480fff1108e1fa1e7573c0 96606e21b18a05245ebd976701bb676dc2962a328d39385ef7571bc48ae134b37410 2030100010282010037b71a3cd838bf0efe65ea9950085b9d4f4d5059d70165cb280 0a975c636f9e7e1d5b27fbfb34b9e459fec2d6cf0998c228f40f567988bc6d6e4c40 a9d04126f1062d8f276d134b36e8a0762df9ce72424c70993fc3955cba7aaa61553d b32f7ff58ce2e0d124f29a7b05c2703e370fb80171d47539988d2c14c37a4802cb1a 7f5685bcc78865480ca4e5d367cafc8b533e610620f94f54a082effc4c4e50998410 dd32fa7dedae895200b56437fe177f47d1b373b5e8e0c62f64b3a19e5918be83e90a 1bbe195a4b516f3ceae6db35b0e4427858631dcbce6b1e49cf12345297df41e54d2c bc2834c34e37bb92888e4659d232a4f3d22edeb9bffa43b7881c7902818100eab3861 80dec393c70c8b00c5fae6a10e6b620ae82e5096ce11bf4c539a015165a7481227e9 1492748159d85317d1e81b780cca1cf19630a10987b940663a2496a4ead2ed4bfb70 17dc813e7a49017aa278b8ac1381ef27fde54ed4alee1e74812dcae514cb9d48590 eb3972b26ba2f21de0aab64cfc1dbcba32561f5f31d6f02818100c062be5756e93eb e005be752a5b7be2d35b342e483ff266cc9f595edbcffff603c8e03dcd9350a19fab f434077f9543088132f0e843c2da6fe4f1cedee49a5eb9a8aea1219a41c1db392521 96137a041def9edcfff43aa9280d90be137dbf48777e6055695f58fcc9cd6b07924fd ab47a5553f5ad7b82d52553f6ec3f647ffe4f0281804221676d2baf1dc97bf5f034e c58d6a6007bdce58f183df9a1cc20c1d9a4d38c42dc84ee553f569f6cde3a4e274d9 be4ecf1abb70405a1345accbc354f3f8fa0a4059b2290eb9c031d8fdc9bee70735a8 c5df330d241560ed574948fc7f7db1521cb70b43791cfb56cf28983d4b2cacf30f9c 183dd99f4839bf3523b31f3d89d0281806cbe63c0928bbcbf410cb1b071a36e87b77 6e034b2b7a24c93cb913794414f64625613b0ddc5b134061bde33ae9cec0d929ce55 85b3e78bf8fb7c02e6d268bf6a4a028b69a6fbcc4bd1fd3f02c9778aa43131a6d152 ba339d491201f7c5086f1a429679dec1b2ca814c88ebb11101a3b9bc79d72b601b9e 12398cae8fa31aed90281810099777cd45f0d1a862888eb2cf7ac14d22d75b88e99a df66f15cccbd29979bf5eaa90bb8c29b29a8be1257425a9a2db2f493df4a740c7fbc 138e4b4d80f24e7ca11d63528d900ba2dd5c44da59e2d601544ec92681161f17b86c 838694a49a978f76ff05287bfce0704c6f3f9fa87551d0cfla970b2cb130b5320783

0105	a36ea8613"/>
0106	</KeyValue>
0107	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0108	<CryptographicLength type="Integer" value="2048"/>
0109	</KeyBlock>
0110	</PrivateKey>
0111	</ResponsePayload>
0112	</BatchItem>
0113	</ResponseMessage>
0113	# TIME 2
0114	<RequestMessage>
0115	<RequestHeader>
0116	<ProtocolVersion>
0117	<ProtocolVersionMajor type="Integer" value="1"/>
0118	<ProtocolVersionMinor type="Integer" value="1"/>
0119	</ProtocolVersion>
0120	<BatchCount type="Integer" value="1"/>
0121	</RequestHeader>
0122	<BatchItem>
0123	<Operation type="Enumeration" value="Get"/>
0124	<RequestPayload>
0125	<UniqueIdentifier type="TextString"
0126	value="\$UNIQUE_IDENTIFIER_1"/>
0127	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0128	</RequestPayload>
0129	</BatchItem>
0130	</RequestMessage>
0131	<ResponseMessage>
0132	<ResponseHeader>
0133	<ProtocolVersion>
0134	<ProtocolVersionMajor type="Integer" value="1"/>
0135	<ProtocolVersionMinor type="Integer" value="1"/>
0136	</ProtocolVersion>
0137	<TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/>
0138	<BatchCount type="Integer" value="1"/>
0139	</ResponseHeader>
0140	<BatchItem>
0141	<Operation type="Enumeration" value="Get"/>
0142	<ResultStatus type="Enumeration" value="Success"/>
0143	<ResponsePayload>
0144	<ObjectType type="Enumeration" value="PublicKey"/>
0145	<UniqueIdentifier type="TextString"
0146	value="\$UNIQUE_IDENTIFIER_1"/>
0147	<PublicKey>
0148	<KeyBlock>
	<KeyFormatType type="Enumeration" value="PKCS_1"/>
	<KeyValue>
	<KeyMaterial type="ByteString"
	value="3082010a0282010100b0612bccafdd11d41819a274526d68dbf3c3f25667c402a0e0e8e4cce007ea6b6ea53699e8bd7ccab7d5ae66c00b28fd678b81bald4e841c3a36caf13f852004633f80d840be7aad9bcdeabde11514b6ab3bce602e11305cf5e9c34ebee32c3c468b9b146502738c0ae82e63ab8bd1fc4db0c6a09eb0c9f6e01b9cc8d22317aedab328209a1dc5d2ce8529d81521c41730c1c8c76249d233e89096ca44dfeb469e3532bb90d6691c6932d0c63dbb7647c6e64337b719a1f100b1366cff3bbb213b17c716beb2c9ad88b3b76abacc378c4898636480fff1108e1fale7573c096606e21b18a05245ebd976701bb676dc2962a328d39385ef7571bc48ae134b37410203010001"/>

0149	</KeyValue>
0150	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0151	<CryptographicLength type="Integer" value="2048"/>
0152	</KeyBlock>
0153	</PublicKey>
0154	</ResponsePayload>
0155	</BatchItem>
0156	</ResponseMessage>
# TIME 3	
0157	<RequestMessage>
0158	<RequestHeader>
0159	<ProtocolVersion>
0160	<ProtocolVersionMajor type="Integer" value="1"/>
0161	<ProtocolVersionMinor type="Integer" value="1"/>
0162	</ProtocolVersion>
0163	<BatchCount type="Integer" value="1"/>
0164	</RequestHeader>
0165	<BatchItem>
0166	<Operation type="Enumeration" value="ReKeyKeyPair"/>
0167	<RequestPayload>
0168	<PrivateKeyUniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0169	</RequestPayload>
0170	</BatchItem>
0171	</RequestMessage>
0172	<ResponseMessage>
0173	<ResponseHeader>
0174	<ProtocolVersion>
0175	<ProtocolVersionMajor type="Integer" value="1"/>
0176	<ProtocolVersionMinor type="Integer" value="1"/>
0177	</ProtocolVersion>
0178	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0179	<BatchCount type="Integer" value="1"/>
0180	</ResponseHeader>
0181	<BatchItem>
0182	<Operation type="Enumeration" value="ReKeyKeyPair"/>
0183	<ResultStatus type="Enumeration" value="Success"/>
0184	<ResponsePayload>
0185	<PrivateKeyUniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0186	<PublicKeyUniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0187	</ResponsePayload>
0188	</BatchItem>
0189	</ResponseMessage>
# TIME 4	
0190	<RequestMessage>
0191	<RequestHeader>
0192	<ProtocolVersion>
0193	<ProtocolVersionMajor type="Integer" value="1"/>
0194	<ProtocolVersionMinor type="Integer" value="1"/>
0195	</ProtocolVersion>
0196	<BatchOrderOption type="Boolean" value="true"/>
0197	<BatchCount type="Integer" value="2"/>
0198	</RequestHeader>
0199	<BatchItem>

0200	<Operation type="Enumeration" value="Locate"/>
0201	<UniqueBatchItemID type="ByteString" value="f409f9adc43f836f"/>
0202	<RequestPayload>
0203	<MaximumItems type="Integer" value="1"/>
0204	<Attribute>
0205	<AttributeName type="TextString" value="Name"/>
0206	<AttributeValue>
0207	<NameValue type="TextString" value="TC-133-11-privateKey1"/>
0208	<NameType type="Enumeration" value="UninterpretedTextString"/>
0209	</AttributeValue>
0210	</Attribute>
0211	<Attribute>
0212	<AttributeName type="TextString" value="Object Type"/>
0213	<AttributeValue type="Enumeration" value="PrivateKey"/>
0214	</Attribute>
0215	</RequestPayload>
0216	</BatchItem>
0217	<BatchItem>
0218	<Operation type="Enumeration" value="Get"/>
0219	<UniqueBatchItemID type="ByteString" value="396c4d8b5bde0667"/>
0220	<RequestPayload>
0221	<KeyFormatType type="Enumeration" value="TransparentRSAPrivateKey"/>
0222	</RequestPayload>
0223	</BatchItem>
0224	</RequestMessage>
0225	<ResponseMessage>
0226	<ResponseHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="1"/>
0230	</ProtocolVersion>
0231	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0232	<BatchCount type="Integer" value="2"/>
0233	</ResponseHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="Locate"/>
0236	<UniqueBatchItemID type="ByteString" value="f409f9adc43f836f"/>
0237	<ResultStatus type="Enumeration" value="Success"/>
0238	<ResponsePayload>
0239	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0240	</ResponsePayload>
0241	</BatchItem>
0242	<BatchItem>
0243	<Operation type="Enumeration" value="Get"/>
0244	<UniqueBatchItemID type="ByteString" value="396c4d8b5bde0667"/>
0245	<ResultStatus type="Enumeration" value="Success"/>
0246	<ResponsePayload>
0247	<ObjectType type="Enumeration" value="PrivateKey"/>
0248	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0249	<PrivateKey>
0250	<KeyBlock>
0251	<KeyFormatType type="Enumeration"

0252	value="TransparentRSAPrivateKey"/>
0253	<KeyValue>
0254	<KeyMaterial>
	<Modulus type="BigInteger"
	value="0000000000000000eab4492bbb2364359408c57b8af47003572c81aaed719 ed92d9b13c741cc196b717d1c98f0c250580e37ac3ade11a7cd1aaede3a0424b53d3 3200510ce7eef71ded7e96e585d1d7ba3767a8dbfad4d2701b5831a34552a827fc2c d398e659fd5063e1dfd28a994b0e6a7449bbad8dcf40e22943b841aa9e58519fa357 5b4409abfeb57f5723b45f7ce4e5277a2d0acccbcd49608d6ff8a7c933d4d70a9e8c 8df24829b58404a5af1b0d4c8668c35e3549e28204f2249bfc13b20c05ab0252c975 e53f604f68c6e498c7b14adb72debac91221a8eb1ad581080144eb8900b4bf9d9792 be37ec6191ad183e2b60b80174eecb66ca08c3ac07f51ba1c056130ec69"/>
0255	<PrivateExponent type="BigInteger"
	value="42e22587e4c86d2227916855907f9ffc13b7872c228622725960bbfe286df 5407d12de376744b8889f64961c20747f911f6d7dbea2b7a33e51776a7a239e60b5d e7f40f2451423f6bbda638a497925675c41519f0212d30e65422a21a0c6ad0993c1d 7e1f0d8829af6dfebd94521cfb56ce1c5c4401d2915531cd804ac0a35ee57d2a43ff d7671aeaad0ab090f17f8419073445ac6fb218bd3c7c5beb9f3e7bf41e4e5f9632d8 492eb0cb2ada41083e040535ae409ad866d1998a0335f253cda2d21a95b2feebacee 64b969aaccab322fa0ecbc75c3f0c15c267dbf431abedecae191b72000b612e41e65 eb93c9f08eef67740b84ba32d9c5697ed91e1c8ccd1"/>
0256	<PublicExponent type="BigInteger"
	value="0000000000010001"/>
0257	<P type="BigInteger"
	value="0000000000000000f88c737435b8b3f5bdb2b2eb73dd5a665e2ee56c64e05 5169038f754ed3021d3e72ae82234dacd4a5fa12edeb4874b70c5915bba4571bef55 964389d8a4b8a79b628771bb4d634fbd18a27ab5fb6973309c4af9e27d269b1c4054 b62012d1c52847e3679f71f91cf7ff6b646c9edaafe5b46845fc1190fa0ef80b8a45 de63973"/>
0258	<Q type="BigInteger"
	value="0000000000000000f1bd952150d189707c316486f205429680230505581b4 0ed503901bef82cec4e2a0a564c58365e8c82b7d34a0305d407194b1d15c273015d1 212969906267322827303b276d0c7585a21ee6758a74e95bfec5b544686325754e5 d2602f0d5734c58f870aa2ca00e08122e940e4d6d0e11611d47966482df8845b8ff8 8d1fbb3"/>
0259	<PrimeExponentP type="BigInteger"
	value="0000000000000000e9717156eac62a305b15a63ac33e5a13dfce0829c0ad7 afd904410f9b1350df0ab247f96f131b8b36c1245a562c5d833793cc77cb290dd1c2 ff393c1540d1368b1905c1ea7c0b14efb45d9707a9b5273db6ee2cb96f767d2511be feb82d34dd0ab24a821f1dbb2e5c3788347058db696e43fdd40da6aa16534cel1f9e3 19b74c5"/>
0260	<PrimeExponentQ type="BigInteger"
	value="0000000000000000eb6294819a364dc3afca507e6dcedd65ba635f1233166 6842d6734e204b989671adc71e768c5980eed819d4525e858ea88a07133ace15ae48 b227a6d8a658a1a823707d49088fe72736132c882b4767aae2518e64633f6c69490b 776b9ca53ad2f1c3add4976a66ac34521019d639adae5e5502352b7900fa49b6f65b 28df4ad"/>
0261	<CRTCoefficient type="BigInteger"
	value="0000000000000000cc75a52cab58eb65878acf7c19070c0a495d5376f40b8 6531b98b1e3b44e28d39db55898db8aa317ce214814efdd00c1d234d4c27168710a1 a68cfdae310f1a56e17e1a51f43d069137beeb7a6aeef4da2b3dfde54d222e24c772 09dc5c8c831b8f09f816d3ee628e76e93bae2594229a59b36ea1f507be2db99ae358 896956e"/>
0262	</KeyMaterial>
0263	</KeyValue>
0264	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0265	<CryptographicLength type="Integer" value="2048"/>

0266	</KeyBlock>
0267	</PrivateKey>
0268	</ResponsePayload>
0269	</BatchItem>
0270	</ResponseMessage>
# TIME 5	
0271	<RequestMessage>
0272	<RequestHeader>
0273	<ProtocolVersion>
0274	<ProtocolVersionMajor type="Integer" value="1"/>
0275	<ProtocolVersionMinor type="Integer" value="1"/>
0276	</ProtocolVersion>
0277	<BatchOrderOption type="Boolean" value="true"/>
0278	<BatchCount type="Integer" value="2"/>
0279	</RequestHeader>
0280	<BatchItem>
0281	<Operation type="Enumeration" value="Locate"/>
0282	<UniqueBatchItemID type="ByteString" value="5df01d7748d64a16"/>
0283	<RequestPayload>
0284	<MaximumItems type="Integer" value="1"/>
0285	<Attribute>
0286	<AttributeName type="TextString" value="Name"/>
0287	<AttributeValue>
0288	<NameValue type="TextString" value="TC-133-11- publicKey1"/>
0289	<NameType type="Enumeration" value="UninterpretedTextString"/>
0290	</AttributeValue>
0291	</Attribute>
0292	<Attribute>
0293	<AttributeName type="TextString" value="Object Type"/>
0294	<AttributeValue type="Enumeration" value="PublicKey"/>
0295	</Attribute>
0296	</RequestPayload>
0297	</BatchItem>
0298	<BatchItem>
0299	<Operation type="Enumeration" value="Get"/>
0300	<UniqueBatchItemID type="ByteString" value="7c7f588280a61c24"/>
0301	<RequestPayload>
0302	<KeyFormatType type="Enumeration" value="TransparentRSAPublicKey"/>
0303	</RequestPayload>
0304	</BatchItem>
0305	</RequestMessage>
0306	<ResponseMessage>
0307	<ResponseHeader>
0308	<ProtocolVersion>
0309	<ProtocolVersionMajor type="Integer" value="1"/>
0310	<ProtocolVersionMinor type="Integer" value="1"/>
0311	</ProtocolVersion>
0312	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0313	<BatchCount type="Integer" value="2"/>
0314	</ResponseHeader>
0315	<BatchItem>
0316	<Operation type="Enumeration" value="Locate"/>
0317	<UniqueBatchItemID type="ByteString" value="5df01d7748d64a16"/>
0318	<ResultStatus type="Enumeration" value="Success"/>

0319	<ResponsePayload>
0320	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0321	</ResponsePayload>
0322	</BatchItem>
0323	<BatchItem>
0324	<Operation type="Enumeration" value="Get"/>
0325	<UniqueBatchItemID type="ByteString" value="7c7f588280a61c24"/>
0326	<ResultStatus type="Enumeration" value="Success"/>
0327	<ResponsePayload>
0328	<ObjectType type="Enumeration" value="PublicKey"/>
0329	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0330	<PublicKey>
0331	<KeyBlock>
0332	<KeyFormatType type="Enumeration"
	value="TransparentRSAPublicKey"/>
0333	<KeyValue>
0334	<KeyMaterial>
0335	<Modulus type="BigInteger"
	value="0000000000000000eab4492bbb2364359408c57b8af47003572c81aaed719
	ed92d9b13c741cc196b717d1c98f0c250580e37ac3ade11a7cd1aaede3a0424b53d3
	3200510ce7eef71ded7e96e585d1d7ba3767a8dbfad4d2701b5831a34552a827fc2c
	d398e659fd5063e1dfd28a994b0e6a7449bbad8dcf40e22943b841aa9e58519fa357
	5b4409abfeb57f5723b45f7ce4e5277a2d0accbcbcd49608d6ff8a7c933d4d70a9e8c
	8df24829b58404a5af1b0d4c8668c35e3549e28204f2249bfc13b20c05ab0252c975
	e53f604f68c6e498c7b14adb72debac91221a8eb1ad581080144eb8900b4bf9d9792
	be37ec6191ad183e2b60b80174eecb66ca08c3ac07f51ba1c056130ec69"/>
0336	<PublicExponent type="BigInteger"
	value="00000000000010001"/>
0337	</KeyMaterial>
0338	</KeyValue>
0339	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0340	<CryptographicLength type="Integer" value="2048"/>
0341	</KeyBlock>
0342	</PublicKey>
0343	</ResponsePayload>
0344	</BatchItem>
0345	</ResponseMessage>
	# TIME 6
0346	<RequestMessage>
0347	<RequestHeader>
0348	<ProtocolVersion>
0349	<ProtocolVersionMajor type="Integer" value="1"/>
0350	<ProtocolVersionMinor type="Integer" value="1"/>
0351	</ProtocolVersion>
0352	<BatchCount type="Integer" value="1"/>
0353	</RequestHeader>
0354	<BatchItem>
0355	<Operation type="Enumeration" value="GetAttributes"/>
0356	<RequestPayload>
0357	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0358	<AttributeName type="TextString" value="Link"/>
0359	</RequestPayload>
0360	</BatchItem>
0361	</RequestMessage>

0362	<ResponseMessage>
0363	<ResponseHeader>
0364	<ProtocolVersion>
0365	<ProtocolVersionMajor type="Integer" value="1"/>
0366	<ProtocolVersionMinor type="Integer" value="1"/>
0367	</ProtocolVersion>
0368	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0369	<BatchCount type="Integer" value="1"/>
0370	</ResponseHeader>
0371	<BatchItem>
0372	<Operation type="Enumeration" value="GetAttributes"/>
0373	<ResultStatus type="Enumeration" value="Success"/>
0374	<ResponsePayload>
0375	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0376	<Attribute>
0377	<AttributeName type="TextString" value="Link"/>
0378	<AttributeValue>
0379	<LinkType type="Enumeration" value="PublicKeyLink"/>
0380	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0381	</AttributeValue>
0382	</Attribute>
0383	<Attribute>
0384	<AttributeName type="TextString" value="Link"/>
0385	<AttributeIndex type="Integer" value="1"/>
0386	<AttributeValue>
0387	<LinkType type="Enumeration" value="ReplacedObjectLink"/>
0388	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0389	</AttributeValue>
0390	</Attribute>
0391	</ResponsePayload>
0392	</BatchItem>
0393	</ResponseMessage>
# TIME 7	
0394	<RequestMessage>
0395	<RequestHeader>
0396	<ProtocolVersion>
0397	<ProtocolVersionMajor type="Integer" value="1"/>
0398	<ProtocolVersionMinor type="Integer" value="1"/>
0399	</ProtocolVersion>
0400	<BatchCount type="Integer" value="1"/>
0401	</RequestHeader>
0402	<BatchItem>
0403	<Operation type="Enumeration" value="GetAttributes"/>
0404	<RequestPayload>
0405	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0406	<AttributeName type="TextString" value="Link"/>
0407	</RequestPayload>
0408	</BatchItem>
0409	</RequestMessage>
0410	<ResponseMessage>
0411	<ResponseHeader>
0412	<ProtocolVersion>
0413	<ProtocolVersionMajor type="Integer" value="1"/>

0414	<ProtocolVersionMinor type="Integer" value="1"/>
0415	</ProtocolVersion>
0416	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0417	<BatchCount type="Integer" value="1"/>
0418	</ResponseHeader>
0419	<BatchItem>
0420	<Operation type="Enumeration" value="GetAttributes"/>
0421	<ResultStatus type="Enumeration" value="Success"/>
0422	<ResponsePayload>
0423	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0424	<Attribute>
0425	<AttributeName type="TextString" value="Link"/>
0426	<AttributeValue>
0427	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0428	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0429	</AttributeValue>
0430	</Attribute>
0431	<Attribute>
0432	<AttributeName type="TextString" value="Link"/>
0433	<AttributeIndex type="Integer" value="1"/>
0434	<AttributeValue>
0435	<LinkType type="Enumeration" value="ReplacedObjectLink"/>
0436	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0437	</AttributeValue>
0438	</Attribute>
0439	</ResponsePayload>
0440	</BatchItem>
0441	</ResponseMessage>
# TIME 8	
0442	<RequestMessage>
0443	<RequestHeader>
0444	<ProtocolVersion>
0445	<ProtocolVersionMajor type="Integer" value="1"/>
0446	<ProtocolVersionMinor type="Integer" value="1"/>
0447	</ProtocolVersion>
0448	<BatchCount type="Integer" value="1"/>
0449	</RequestHeader>
0450	<BatchItem>
0451	<Operation type="Enumeration" value="GetAttributes"/>
0452	<RequestPayload>
0453	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0454	<AttributeName type="TextString" value="Link"/>
0455	</RequestPayload>
0456	</BatchItem>
0457	</RequestMessage>
0458	<ResponseMessage>
0459	<ResponseHeader>
0460	<ProtocolVersion>
0461	<ProtocolVersionMajor type="Integer" value="1"/>
0462	<ProtocolVersionMinor type="Integer" value="1"/>
0463	</ProtocolVersion>
0464	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0465	<BatchCount type="Integer" value="1"/>

0466	</ResponseHeader>
0467	<BatchItem>
0468	<Operation type="Enumeration" value="GetAttributes"/>
0469	<ResultStatus type="Enumeration" value="Success"/>
0470	<ResponsePayload>
0471	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0472	<Attribute>
0473	<AttributeName type="TextString" value="Link"/>
0474	<AttributeValue>
0475	<LinkType type="Enumeration" value="PublicKeyLink"/>
0476	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0477	</AttributeValue>
0478	</Attribute>
0479	<Attribute>
0480	<AttributeName type="TextString" value="Link"/>
0481	<AttributeIndex type="Integer" value="1"/>
0482	<AttributeValue>
0483	<LinkType type="Enumeration"
	value="ReplacementObjectLink"/>
0484	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0485	</AttributeValue>
0486	</Attribute>
0487	</ResponsePayload>
0488	</BatchItem>
0489	</ResponseMessage>
	# TIME 9
0490	<RequestMessage>
0491	<RequestHeader>
0492	<ProtocolVersion>
0493	<ProtocolVersionMajor type="Integer" value="1"/>
0494	<ProtocolVersionMinor type="Integer" value="1"/>
0495	</ProtocolVersion>
0496	<BatchCount type="Integer" value="1"/>
0497	</RequestHeader>
0498	<BatchItem>
0499	<Operation type="Enumeration" value="GetAttributes"/>
0500	<RequestPayload>
0501	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0502	<AttributeName type="TextString" value="Link"/>
0503	</RequestPayload>
0504	</BatchItem>
0505	</RequestMessage>
0506	<ResponseMessage>
0507	<ResponseHeader>
0508	<ProtocolVersion>
0509	<ProtocolVersionMajor type="Integer" value="1"/>
0510	<ProtocolVersionMinor type="Integer" value="1"/>
0511	</ProtocolVersion>
0512	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0513	<BatchCount type="Integer" value="1"/>
0514	</ResponseHeader>
0515	<BatchItem>
0516	<Operation type="Enumeration" value="GetAttributes"/>

0517	<ResultStatus type="Enumeration" value="Success"/>
0518	<ResponsePayload>
0519	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0520	<Attribute>
0521	<AttributeName type="TextString" value="Link"/>
0522	<AttributeValue>
0523	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0524	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0525	</AttributeValue>
0526	</Attribute>
0527	<Attribute>
0528	<AttributeName type="TextString" value="Link"/>
0529	<AttributeIndex type="Integer" value="1"/>
0530	<AttributeValue>
0531	<LinkType type="Enumeration"
	value="ReplacementObjectLink"/>
0532	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0533	</AttributeValue>
0534	</Attribute>
0535	</ResponsePayload>
0536	</BatchItem>
0537	</ResponseMessage>
# TIME 10	
0538	<RequestMessage>
0539	<RequestHeader>
0540	<ProtocolVersion>
0541	<ProtocolVersionMajor type="Integer" value="1"/>
0542	<ProtocolVersionMinor type="Integer" value="1"/>
0543	</ProtocolVersion>
0544	<BatchCount type="Integer" value="1"/>
0545	</RequestHeader>
0546	<BatchItem>
0547	<Operation type="Enumeration" value="Destroy"/>
0548	<RequestPayload>
0549	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0550	</RequestPayload>
0551	</BatchItem>
0552	</RequestMessage>
0553	<ResponseMessage>
0554	<ResponseHeader>
0555	<ProtocolVersion>
0556	<ProtocolVersionMajor type="Integer" value="1"/>
0557	<ProtocolVersionMinor type="Integer" value="1"/>
0558	</ProtocolVersion>
0559	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0560	<BatchCount type="Integer" value="1"/>
0561	</ResponseHeader>
0562	<BatchItem>
0563	<Operation type="Enumeration" value="Destroy"/>
0564	<ResultStatus type="Enumeration" value="Success"/>
0565	<ResponsePayload>
0566	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0567	</ResponsePayload>
0568	</BatchItem>
0569	</ResponseMessage>
# TIME 11	
0570	<RequestMessage>
0571	<RequestHeader>
0572	<ProtocolVersion>
0573	<ProtocolVersionMajor type="Integer" value="1"/>
0574	<ProtocolVersionMinor type="Integer" value="1"/>
0575	</ProtocolVersion>
0576	<BatchCount type="Integer" value="1"/>
0577	</RequestHeader>
0578	<BatchItem>
0579	<Operation type="Enumeration" value="Destroy"/>
0580	<RequestPayload>
0581	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0582	</RequestPayload>
0583	</BatchItem>
0584	</RequestMessage>
0585	<ResponseMessage>
0586	<ResponseHeader>
0587	<ProtocolVersion>
0588	<ProtocolVersionMajor type="Integer" value="1"/>
0589	<ProtocolVersionMinor type="Integer" value="1"/>
0590	</ProtocolVersion>
0591	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0592	<BatchCount type="Integer" value="1"/>
0593	</ResponseHeader>
0594	<BatchItem>
0595	<Operation type="Enumeration" value="Destroy"/>
0596	<ResultStatus type="Enumeration" value="Success"/>
0597	<ResponsePayload>
0598	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0599	</ResponsePayload>
0600	</BatchItem>
0601	</ResponseMessage>
# TIME 12	
0602	<RequestMessage>
0603	<RequestHeader>
0604	<ProtocolVersion>
0605	<ProtocolVersionMajor type="Integer" value="1"/>
0606	<ProtocolVersionMinor type="Integer" value="1"/>
0607	</ProtocolVersion>
0608	<BatchCount type="Integer" value="1"/>
0609	</RequestHeader>
0610	<BatchItem>
0611	<Operation type="Enumeration" value="Destroy"/>
0612	<RequestPayload>
0613	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0614	</RequestPayload>
0615	</BatchItem>
0616	</RequestMessage>
0617	<ResponseMessage>

0618	<ResponseHeader>
0619	<ProtocolVersion>
0620	<ProtocolVersionMajor type="Integer" value="1"/>
0621	<ProtocolVersionMinor type="Integer" value="1"/>
0622	</ProtocolVersion>
0623	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0624	<BatchCount type="Integer" value="1"/>
0625	</ResponseHeader>
0626	<BatchItem>
0627	<Operation type="Enumeration" value="Destroy"/>
0628	<ResultStatus type="Enumeration" value="Success"/>
0629	<ResponsePayload>
0630	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0631	</ResponsePayload>
0632	</BatchItem>
0633	</ResponseMessage>
# TIME 13	
0634	<RequestMessage>
0635	<RequestHeader>
0636	<ProtocolVersion>
0637	<ProtocolVersionMajor type="Integer" value="1"/>
0638	<ProtocolVersionMinor type="Integer" value="1"/>
0639	</ProtocolVersion>
0640	<BatchCount type="Integer" value="1"/>
0641	</RequestHeader>
0642	<BatchItem>
0643	<Operation type="Enumeration" value="Destroy"/>
0644	<RequestPayload>
0645	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0646	</RequestPayload>
0647	</BatchItem>
0648	</RequestMessage>
0649	<ResponseMessage>
0650	<ResponseHeader>
0651	<ProtocolVersion>
0652	<ProtocolVersionMajor type="Integer" value="1"/>
0653	<ProtocolVersionMinor type="Integer" value="1"/>
0654	</ProtocolVersion>
0655	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0656	<BatchCount type="Integer" value="1"/>
0657	</ResponseHeader>
0658	<BatchItem>
0659	<Operation type="Enumeration" value="Destroy"/>
0660	<ResultStatus type="Enumeration" value="Success"/>
0661	<ResponsePayload>
0662	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0663	</ResponsePayload>
0664	</BatchItem>
0665	</ResponseMessage>

530 2.2.27 TC-134-11 - Register Key Pair, Certify and Re-certify Public Key

531 Register a public/private key pair on the server. Request the server to have a certificate created
532 using the Certify operation. Retrieve the certificate and its attributes, then execute the Re-
533 certify operation to re-certify the public key. Finally, destroy all the objects.

534 The new KMIP 1.1 certificate DN attributes are retrieved as are the original (deprecated) KMIP
535 1.0 certificate DN attributes.

```
# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="1"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="Register"/>
0011     <RequestPayload>
0012       <ObjectType type="Enumeration" value="PublicKey"/>
0013       <TemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0016           <AttributeValue type="Integer" value="Verify"/>
0017         </Attribute>
0018         <Attribute>
0019           <AttributeName type="TextString" value="x-ID"/>
0020           <AttributeValue type="TextString" value="TC-134-11-
pubkey1"/>
0021         </Attribute>
0022       </TemplateAttribute>
0023       <PublicKey>
0024         <KeyBlock>
0025           <KeyFormatType type="Enumeration" value="PKCS_1"/>
0026           <KeyValue>
0027             <KeyMaterial type="ByteString"
value="3082010a0282010100ab7f161c0042496ccd6c6d4dad9199734353577760
03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b
8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89
b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981
35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328
abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013
da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612
a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010
001"/>
0028           </KeyValue>
0029           <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0030           <CryptographicLength type="Integer" value="2048"/>
0031         </KeyBlock>
0032       </PublicKey>
0033     </RequestPayload>
0034   </BatchItem>
0035 </RequestMessage>
```

0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="1"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="1"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PrivateKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0068	<AttributeValue type="Integer" value="Sign"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>
0073	<LinkType type="Enumeration" value="PublicKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0075	</AttributeValue>
0076	</Attribute>
0077	</TemplateAttribute>
0078	<Attribute>
0079	<AttributeName type="TextString" value="x-ID"/>
	<AttributeValue type="TextString" value="TC-134-11-
	prikey1"/>
0080	</Attribute>
0081	</RequestPayload>
0082	<PrivateKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString"
	value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353

	57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618fa74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0aa49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8c3cdc2464744a793713dafb9f1dbcb799ff96423fecdd3cba794286bce920f4b5c183f99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d5659674c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04cec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0e94adlee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920dbe22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aaelebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee27d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eae9a922fd75d5b16b1a561fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a726a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d349417e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f8129c32341a8b44f"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0089	<CryptographicLength type="Integer" value="2048"/>
0090	</KeyBlock>
0091	</PrivateKey>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="1"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString"

0109	value="\$UNIQUE_IDENTIFIER_1"/>
0110	</ResponsePayload>
0111	</BatchItem>
0112	</ResponseMessage>
# TIME 2	
0112	<RequestMessage>
0113	<RequestHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="1"/>
0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="AddAttribute"/>
0122	<RequestPayload>
0123	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Link"/>
0126	<AttributeValue>
0127	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0128	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0129	</AttributeValue>
0130	</Attribute>
0131	</RequestPayload>
0132	</BatchItem>
0133	</RequestMessage>
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="1"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="AddAttribute"/>
0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0148	<Attribute>
0149	<AttributeName type="TextString" value="Link"/>
0150	<AttributeValue>
0151	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0152	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0153	</AttributeValue>
0154	</Attribute>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
# TIME 3	

0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="1"/>
0163	</ProtocolVersion>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Certify"/>
0168	<RequestPayload>
0169	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0170	<CertificateRequestType type="Enumeration" value="PKCS_10"/>
0171	<CertificateRequest type="ByteString"
	value="3082028130820169020100303c310b3009060355040613025553310d300b0
	60355040a130441434d45310d300b060355040b13044b4d4950310f300d060355040
	31306436c69656e7430820122300d06092a864886f70d01010105000382010f00308
	2010a0282010100ab7f161c0042496ccd6c6d4dad919973435357776003acf54b7a
	f1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b8d71812b20
	5387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89b9bee9e60a
	1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f98135b1c67b70
	1675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328abf70e1b42
	e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da809e9c1b
	7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a29a82d73a
	1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010001a000300
	d06092a864886f70d010105050003820101002d90f5492c3df1771df4e87e1087cb9
	52197319a9696e2d588efda580d8d3304427b997cd921ad7c674aea413fba85fd61e
	6a481de9ab2e8a4ff43c02655015d3437f783fe0c781519cd08ffd3c007c7fade963
	2fe5659e2cac35bd6aaf3e13dc18097d996df01b66fc5e26ca109380863a209125cc
	0fd79533f327falcad444d89d3ff81b92a91428c469c846090fd1324846e12d01671
	962c332a7826152daaf486cc867185c2e27caf2f009898db07fe4b45c518192aa493
	d8f8c0198db67f90672ab6de05a08032941377f473d80716d85adc6182003ab34942
	302214eb3895f15403f2616adfd6bb5e6aa47fa38c9dfc73f4de80ddb91bdb04d21c
	82ba6"/>
0172	<TemplateAttribute>
0173	<Attribute>
0174	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0175	<AttributeValue type="Integer" value="Verify Sign"/>
0176	</Attribute>
0177	</Attribute>
0178	<AttributeName type="TextString" value="Name"/>
0179	<AttributeValue>
0180	<NameValue type="TextString" value="TC-134-11-
	certificatel"/>
0181	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0182	</AttributeValue>
0183	</Attribute>
0184	</TemplateAttribute>
0185	</RequestPayload>
0186	</BatchItem>
0187	</RequestMessage>
0188	<ResponseMessage>
0189	<ResponseHeader>
0190	<ProtocolVersion>

0191	<ProtocolVersionMajor type="Integer" value="1"/>
0192	<ProtocolVersionMinor type="Integer" value="1"/>
0193	</ProtocolVersion>
0194	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0195	<BatchCount type="Integer" value="1"/>
0196	</ResponseHeader>
0197	<BatchItem>
0198	<Operation type="Enumeration" value="Certify"/>
0199	<ResultStatus type="Enumeration" value="Success"/>
0200	<ResponsePayload>
0201	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0202	</ResponsePayload>
0203	</BatchItem>
0204	</ResponseMessage>
# TIME 4	
0205	<RequestMessage>
0206	<RequestHeader>
0207	<ProtocolVersion>
0208	<ProtocolVersionMajor type="Integer" value="1"/>
0209	<ProtocolVersionMinor type="Integer" value="1"/>
0210	</ProtocolVersion>
0211	<BatchCount type="Integer" value="1"/>
0212	</RequestHeader>
0213	<BatchItem>
0214	<Operation type="Enumeration" value="Get"/>
0215	<RequestPayload>
0216	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0217	</RequestPayload>
0218	</BatchItem>
0219	</RequestMessage>
0220	<ResponseMessage>
0221	<ResponseHeader>
0222	<ProtocolVersion>
0223	<ProtocolVersionMajor type="Integer" value="1"/>
0224	<ProtocolVersionMinor type="Integer" value="1"/>
0225	</ProtocolVersion>
0226	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0227	<BatchCount type="Integer" value="1"/>
0228	</ResponseHeader>
0229	<BatchItem>
0230	<Operation type="Enumeration" value="Get"/>
0231	<ResultStatus type="Enumeration" value="Success"/>
0232	<ResponsePayload>
0233	<ObjectType type="Enumeration" value="Certificate"/>
0234	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0235	<Certificate>
0236	<CertificateType type="Enumeration" value="X_509"/>
0237	<CertificateValue type="ByteString"
	value="30820277308201e0a0030201020209009bba23d1b6a48f97300d06092a864886f70d01010b0500303b310b3009060355040613025553310d300b060355040a130454455354310e300c060355040b13054f41534953310d300b060355040313044b4d4950301e170d3133303631383038353535375a170d3134303631383038353535375a303c310b3009060355040613025553310d300b060355040a130441434d45310d300b060355040b13044b4d4950310f300d06035504031306436c69656e7430820122300d0

0238	6092a864886f70d01010105000382010f003082010a0282010100ab7f161c0042496
0239	ccd6c6d4dadb919973435357776003acf54b7af1e440afb80b64a8755f8002cfeba6
0240	b184540a2d66086d74648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176
0241	b7957c422e7d03fc6267fa2a6f89b9bee9e60ald7c2d833e5a5f4bb0b1434f4e795a
	41100f8aa214900df8b65089f98135b1c67b701675abdbc7d5721aac9d14a7f081fc
	ec80b64e8a0ecc8295353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d2112
	6eba8da7d0ca34142cb76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c
	8d7cce8946a9ac99b1c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6f
	c411335d5dc7426b0f6050203010001300d06092a864886f70d01010b05000381810
	0c4fe08d5bd74239648c7faabaed0978527ac01a0fd17b8a65c0d92501c4eab3f487
	511062eafedc1024e74dc6bfdaae7f66d1fdda7574f6db3f03c6de83586b52c593a4
	671001a0531bc43eff4849880b07924b7a9a0236d5d64d82d4d8e42dcd3a72c80728
	804f9ba7f0e80c3fe3eb09cb3ed7fbfb2167c99be513ff9db0b6"/>
	</Certificate>
	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>
0242	# TIME 5
0243	<RequestMessage>
0244	<RequestHeader>
0245	<ProtocolVersion>
0246	<ProtocolVersionMajor type="Integer" value="1"/>
0247	<ProtocolVersionMinor type="Integer" value="1"/>
0248	</ProtocolVersion>
0249	<BatchCount type="Integer" value="1"/>
0250	</RequestHeader>
0251	<BatchItem>
0252	<Operation type="Enumeration" value="GetAttributeList"/>
0253	<RequestPayload>
0254	<UniqueIdentifier type="TextString"
0255	value="\$UNIQUE_IDENTIFIER_2"/>
0256	</RequestPayload>
0257	</BatchItem>
0258	</RequestMessage>
0259	<ResponseMessage>
0260	<ResponseHeader>
0261	<ProtocolVersion>
0262	<ProtocolVersionMajor type="Integer" value="1"/>
0263	<ProtocolVersionMinor type="Integer" value="1"/>
0264	</ProtocolVersion>
0265	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0266	<BatchCount type="Integer" value="1"/>
0267	</ResponseHeader>
0268	<BatchItem>
0269	<Operation type="Enumeration" value="GetAttributeList"/>
0270	<ResultStatus type="Enumeration" value="Success"/>
0271	<ResponsePayload>
0272	<UniqueIdentifier type="TextString"
0273	value="\$UNIQUE_IDENTIFIER_2"/>
0274	<AttributeName type="TextString" value="Cryptographic
0275	Length"/>
	<AttributeName type="TextString" value="Certificate Length"/>
	<AttributeName type="TextString" value="X.509 Certificate
	Identifier"/>
	<AttributeName type="TextString" value="X.509 Certificate
	Issuer"/>
	<AttributeName type="TextString" value="X.509 Certificate

0276	Subject"/>
0277	<AttributeName type="TextString" value="Digital Signature
0278	Algorithm"/>
0279	<AttributeName type="TextString" value="Fresh"/>
0280	<AttributeName type="TextString" value="Certificate Issuer"/>
0281	<AttributeName type="TextString" value="Certificate Type"/>
0282	<AttributeName type="TextString" value="Certificate Subject"/>
0283	<AttributeName type="TextString" value="Certificate
0284	Identifier"/>
0285	<AttributeName type="TextString" value="State"/>
0286	<AttributeName type="TextString" value="Digest"/>
0287	<AttributeName type="TextString" value="Link"/>
0288	<AttributeName type="TextString" value="Lease Time"/>
0289	<AttributeName type="TextString" value="Initial Date"/>
0290	<AttributeName type="TextString" value="Unique Identifier"/>
0291	<AttributeName type="TextString" value="Name"/>
0292	<AttributeName type="TextString" value="Cryptographic Usage
0293	Mask"/>
0294	<AttributeName type="TextString" value="Object Type"/>
0295	<AttributeName type="TextString" value="Last Change Date"/>
0296	</ResponsePayload>
0297	</BatchItem>
0298	</ResponseMessage>
0299	# TIME 6
0300	<RequestMessage>
0301	<RequestHeader>
0302	<ProtocolVersion>
0303	<ProtocolVersionMajor type="Integer" value="1"/>
0304	<ProtocolVersionMinor type="Integer" value="1"/>
0305	</ProtocolVersion>
0306	<BatchCount type="Integer" value="1"/>
0307	</RequestHeader>
0308	<BatchItem>
0309	<Operation type="Enumeration" value="GetAttributes"/>
0310	<RequestPayload>
0311	<UniqueIdentifier type="TextString"
0312	value="\$UNIQUE_IDENTIFIER 2"/>
0313	<AttributeName type="TextString" value="Certificate
0314	Identifier"/>
0315	<AttributeName type="TextString" value="Certificate Issuer"/>
0316	<AttributeName type="TextString" value="Certificate Subject"/>
0317	<AttributeName type="TextString" value="Certificate Type"/>
0318	<AttributeName type="TextString" value="Digital Signature
0319	Algorithm"/>
0320	<AttributeName type="TextString" value="Cryptographic
0321	Length"/>
0322	<AttributeName type="TextString" value="Certificate Length"/>
0323	<AttributeName type="TextString" value="X.509 Certificate
0324	Identifier"/>
0325	<AttributeName type="TextString" value="X.509 Certificate
0326	Issuer"/>
0327	<AttributeName type="TextString" value="X.509 Certificate
0328	Subject"/>
0329	</RequestPayload>
0330	</BatchItem>
0331	</RequestMessage>
0332	<ResponseMessage>

```
0321 <ResponseHeader>
0322   <ProtocolVersion>
0323     <ProtocolVersionMajor type="Integer" value="1"/>
0324     <ProtocolVersionMinor type="Integer" value="1"/>
0325   </ProtocolVersion>
0326   <TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0327   <BatchCount type="Integer" value="1"/>
0328 </ResponseHeader>
0329 <BatchItem>
0330   <Operation type="Enumeration" value="GetAttributes"/>
0331   <ResultStatus type="Enumeration" value="Success"/>
0332   <ResponsePayload>
0333     <UniqueIdentifier type="TextString"
0334       value="$UNIQUE_IDENTIFIER_2"/>
0335     <Attribute>
0336       <AttributeName type="TextString" value="Certificate
0337       Identifier"/>
0338       <AttributeValue>
0339         <Issuer type="TextString"
0340         value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0341         <SerialNumber type="TextString" value="9BBA23D1B6A48F97"/>
0342       </AttributeValue>
0343     </Attribute>
0344     <Attribute>
0345       <AttributeName type="TextString" value="Certificate
0346       Issuer"/>
0347       <AttributeValue>
0348         <CertificateIssuerDistinguishedName type="TextString"
0349         value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0350       </AttributeValue>
0351     </Attribute>
0352     <Attribute>
0353       <AttributeName type="TextString" value="Certificate
0354       Subject"/>
0355       <AttributeValue>
0356         <CertificateSubjectDistinguishedName type="TextString"
0357         value="CN=Client,OU=KMIP,O=ACME,C=US"/>
0358       </AttributeValue>
0359     </Attribute>
0360     <Attribute>
0361       <AttributeName type="TextString" value="Certificate Type"/>
0362       <AttributeValue type="Enumeration" value="X_509"/>
0363     </Attribute>
0364     <Attribute>
0365       <AttributeName type="TextString" value="Digital Signature
0366       Algorithm"/>
0367       <AttributeValue type="Enumeration"
0368       value="SHA_256WithRSAEncryption"/>
0369     </Attribute>
0370     <Attribute>
0371       <AttributeName type="TextString" value="Cryptographic
0372       Length"/>
0373       <AttributeValue type="Integer" value="2048"/>
0374     </Attribute>
0375     <Attribute>
0376       <AttributeName type="TextString" value="Certificate
0377       Length"/>
```

0367	<AttributeValue type="Integer" value="635"/>
0368	</Attribute>
0369	<Attribute>
0370	<AttributeName type="TextString" value="X.509 Certificate Identifier"/>
0371	<AttributeValue>
0372	<IssuerDistinguishedName type="ByteString" value="303b310b3009060355040613025553310d300b060355040a130454455354310e300c060355040b13054f41534953310d300b060355040313044b4d4950"/>
0373	<CertificateSerialNumber type="ByteString" value="0209009bba23d1b6a48f97"/>
0374	</AttributeValue>
0375	</Attribute>
0376	<Attribute>
0377	<AttributeName type="TextString" value="X.509 Certificate Issuer"/>
0378	<AttributeValue>
0379	<IssuerDistinguishedName type="ByteString" value="303b310b3009060355040613025553310d300b060355040a130454455354310e300c060355040b13054f41534953310d300b060355040313044b4d4950"/>
0380	</AttributeValue>
0381	</Attribute>
0382	<Attribute>
0383	<AttributeName type="TextString" value="X.509 Certificate Subject"/>
0384	<AttributeValue>
0385	<SubjectDistinguishedName type="ByteString" value="303c310b3009060355040613025553310d300b060355040a130441434d45310d300b060355040b13044b4d4950310f300d06035504031306436c69656e74"/>
0386	</AttributeValue>
0387	</Attribute>
0388	</ResponsePayload>
0389	</BatchItem>
0390	</ResponseMessage>
	# TIME 7
0391	<RequestMessage>
0392	<RequestHeader>
0393	<ProtocolVersion>
0394	<ProtocolVersionMajor type="Integer" value="1"/>
0395	<ProtocolVersionMinor type="Integer" value="1"/>
0396	</ProtocolVersion>
0397	<BatchCount type="Integer" value="1"/>
0398	</RequestHeader>
0399	<BatchItem>
0400	<Operation type="Enumeration" value="ReCertify"/>
0401	<RequestPayload>
0402	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0403	<CertificateRequestType type="Enumeration" value="PKCS_10"/>
0404	<CertificateRequest type="ByteString" value="3082028130820169020100303c310b3009060355040613025553310d300b060355040a130441434d45310d300b060355040b13044b4d4950310f300d06035504031306436c69656e7430820122300d06092a864886f70d01010105000382010f003082010a0282010100ab7f161c0042496ccd6c6d4dad919973435357776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f98135b1c67b70

	1675abdbbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010001a000300d06092a864886f70d010105050003820101002d90f5492c3df1771df4e87e1087cb952197319a9696e2d588efda580d8d3304427b997cd921ad7c674aea413fba85fd61e6a481de9ab2e8a4ff43c02655015d3437f783fe0c781519cd08ffd3c007c7fade9632fe5659e2cac35bd6aaf3e13dc18097d996df01b66fc5e26ca109380863a209125cc0fd79533f327falcad444d89d3ff81b92a91428c469c846090fd1324846e12d01671962c332a7826152daaf486cc867185c2e27caf2f009898db07fe4b45c518192aa493d8f8c0198db67f90672ab6de05a08032941377f473d80716d85adc6182003ab34942302214eb3895f15403f2616adfd6bb5e6aa47fa38c9dfc73f4de80ddb91bdb04d21c82ba6"/>
0405	<TemplateAttribute>
0406	<Attribute>
0407	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0408	<AttributeValue type="Integer" value="Verify Sign"/>
0409	</Attribute>
0410	<Attribute>
0411	<AttributeName type="TextString" value="Name"/>
0412	<AttributeValue>
0413	<NameValue type="TextString" value="TC-134-11-certificate2"/>
0414	<NameType type="Enumeration" value="UninterpretedTextString"/>
0415	</AttributeValue>
0416	</Attribute>
0417	</TemplateAttribute>
0418	</RequestPayload>
0419	</BatchItem>
0420	</RequestMessage>
0421	<ResponseMessage>
0422	<ResponseHeader>
0423	<ProtocolVersion>
0424	<ProtocolVersionMajor type="Integer" value="1"/>
0425	<ProtocolVersionMinor type="Integer" value="1"/>
0426	</ProtocolVersion>
0427	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0428	<BatchCount type="Integer" value="1"/>
0429	</ResponseHeader>
0430	<BatchItem>
0431	<Operation type="Enumeration" value="ReCertify"/>
0432	<ResultStatus type="Enumeration" value="Success"/>
0433	<ResponsePayload>
0434	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_3"/>
0435	</ResponsePayload>
0436	</BatchItem>
0437	</ResponseMessage>
	# TIME 8
0438	<RequestMessage>
0439	<RequestHeader>
0440	<ProtocolVersion>
0441	<ProtocolVersionMajor type="Integer" value="1"/>
0442	<ProtocolVersionMinor type="Integer" value="1"/>
0443	</ProtocolVersion>

0444	<BatchCount type="Integer" value="1"/>
0445	</RequestHeader>
0446	<BatchItem>
0447	<Operation type="Enumeration" value="GetAttributes"/>
0448	<RequestPayload>
0449	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0450	<AttributeName type="TextString" value="Link"/>
0451	</RequestPayload>
0452	</BatchItem>
0453	</RequestMessage>
0454	<ResponseMessage>
0455	<ResponseHeader>
0456	<ProtocolVersion>
0457	<ProtocolVersionMajor type="Integer" value="1"/>
0458	<ProtocolVersionMinor type="Integer" value="1"/>
0459	</ProtocolVersion>
0460	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0461	<BatchCount type="Integer" value="1"/>
0462	</ResponseHeader>
0463	<BatchItem>
0464	<Operation type="Enumeration" value="GetAttributes"/>
0465	<ResultStatus type="Enumeration" value="Success"/>
0466	<ResponsePayload>
0467	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0468	<Attribute>
0469	<AttributeName type="TextString" value="Link"/>
0470	<AttributeValue>
0471	<LinkType type="Enumeration" value="PublicKeyLink"/>
0472	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0473	</AttributeValue>
0474	</Attribute>
0475	</ResponsePayload>
0476	</BatchItem>
0477	</ResponseMessage>
	# TIME 9
0478	<RequestMessage>
0479	<RequestHeader>
0480	<ProtocolVersion>
0481	<ProtocolVersionMajor type="Integer" value="1"/>
0482	<ProtocolVersionMinor type="Integer" value="1"/>
0483	</ProtocolVersion>
0484	<BatchCount type="Integer" value="1"/>
0485	</RequestHeader>
0486	<BatchItem>
0487	<Operation type="Enumeration" value="GetAttributes"/>
0488	<RequestPayload>
0489	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0490	<AttributeName type="TextString" value="Link"/>
0491	</RequestPayload>
0492	</BatchItem>
0493	</RequestMessage>
0494	<ResponseMessage>

0495	<ResponseHeader>
0496	<ProtocolVersion>
0497	<ProtocolVersionMajor type="Integer" value="1"/>
0498	<ProtocolVersionMinor type="Integer" value="1"/>
0499	</ProtocolVersion>
0500	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0501	<BatchCount type="Integer" value="1"/>
0502	</ResponseHeader>
0503	<BatchItem>
0504	<Operation type="Enumeration" value="GetAttributes"/>
0505	<ResultStatus type="Enumeration" value="Success"/>
0506	<ResponsePayload>
0507	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0508	<Attribute>
0509	<AttributeName type="TextString" value="Link"/>
0510	<AttributeValue>
0511	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0512	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0513	</AttributeValue>
0514	</Attribute>
0515	<Attribute>
0516	<AttributeName type="TextString" value="Link"/>
0517	<AttributeIndex type="Integer" value="1"/>
0518	<AttributeValue>
0519	<LinkType type="Enumeration" value="CertificateLink"/>
0520	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0521	</AttributeValue>
0522	</Attribute>
0523	</ResponsePayload>
0524	</BatchItem>
0525	</ResponseMessage>
	# TIME 10
0526	<RequestMessage>
0527	<RequestHeader>
0528	<ProtocolVersion>
0529	<ProtocolVersionMajor type="Integer" value="1"/>
0530	<ProtocolVersionMinor type="Integer" value="1"/>
0531	</ProtocolVersion>
0532	<BatchCount type="Integer" value="1"/>
0533	</RequestHeader>
0534	<BatchItem>
0535	<Operation type="Enumeration" value="GetAttributes"/>
0536	<RequestPayload>
0537	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0538	<AttributeName type="TextString" value="Link"/>
0539	</RequestPayload>
0540	</BatchItem>
0541	</RequestMessage>
0542	<ResponseMessage>
0543	<ResponseHeader>
0544	<ProtocolVersion>
0545	<ProtocolVersionMajor type="Integer" value="1"/>
0546	<ProtocolVersionMinor type="Integer" value="1"/>

0547	</ProtocolVersion>
0548	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0549	<BatchCount type="Integer" value="1"/>
0550	</ResponseHeader>
0551	<BatchItem>
0552	<Operation type="Enumeration" value="GetAttributes"/>
0553	<ResultStatus type="Enumeration" value="Success"/>
0554	<ResponsePayload>
0555	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0556	<Attribute>
0557	<AttributeName type="TextString" value="Link"/>
0558	<AttributeValue>
0559	<LinkType type="Enumeration" value="PublicKeyLink"/>
0560	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0561	</AttributeValue>
0562	</Attribute>
0563	<Attribute>
0564	<AttributeName type="TextString" value="Link"/>
0565	<AttributeIndex type="Integer" value="1"/>
0566	<AttributeValue>
0567	<LinkType type="Enumeration"
	value="ReplacementObjectLink"/>
0568	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0569	</AttributeValue>
0570	</Attribute>
0571	</ResponsePayload>
0572	</BatchItem>
0573	</ResponseMessage>
# TIME 11	
0574	<RequestMessage>
0575	<RequestHeader>
0576	<ProtocolVersion>
0577	<ProtocolVersionMajor type="Integer" value="1"/>
0578	<ProtocolVersionMinor type="Integer" value="1"/>
0579	</ProtocolVersion>
0580	<BatchCount type="Integer" value="1"/>
0581	</RequestHeader>
0582	<BatchItem>
0583	<Operation type="Enumeration" value="GetAttributes"/>
0584	<RequestPayload>
0585	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0586	<AttributeName type="TextString" value="Link"/>
0587	<AttributeName type="TextString" value="Certificate
	Identifier"/>
0588	<AttributeName type="TextString" value="Name"/>
0589	</RequestPayload>
0590	</BatchItem>
0591	</RequestMessage>
0592	<ResponseMessage>
0593	<ResponseHeader>
0594	<ProtocolVersion>
0595	<ProtocolVersionMajor type="Integer" value="1"/>
0596	<ProtocolVersionMinor type="Integer" value="1"/>

```

0597     </ProtocolVersion>
0598     <TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0599     <BatchCount type="Integer" value="1"/>
0600 </ResponseHeader>
0601 <BatchItem>
0602     <Operation type="Enumeration" value="GetAttributes"/>
0603     <ResultStatus type="Enumeration" value="Success"/>
0604     <ResponsePayload>
0605         <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_3"/>
0606         <Attribute>
0607             <AttributeName type="TextString" value="Link"/>
0608             <AttributeValue>
0609                 <LinkType type="Enumeration" value="ReplacedObjectLink"/>
0610                 <LinkedObjectIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_2"/>
0611             </AttributeValue>
0612         </Attribute>
0613         <Attribute>
0614             <AttributeName type="TextString" value="Link"/>
0615             <AttributeIndex type="Integer" value="1"/>
0616             <AttributeValue>
0617                 <LinkType type="Enumeration" value="PublicKeyLink"/>
0618                 <LinkedObjectIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0619             </AttributeValue>
0620         </Attribute>
0621         <Attribute>
0622             <AttributeName type="TextString" value="Certificate
Identifier"/>
0623             <AttributeValue>
0624                 <Issuer type="TextString"
value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0625                 <SerialNumber type="TextString" value="CF77F7A23282BC12"/>
0626             </AttributeValue>
0627         </Attribute>
0628         <Attribute>
0629             <AttributeName type="TextString" value="Name"/>
0630             <AttributeValue>
0631                 <NameValue type="TextString" value="TC-134-11-
certificate1"/>
0632                 <NameType type="Enumeration"
value="UninterpretedTextString"/>
0633             </AttributeValue>
0634         </Attribute>
0635         <Attribute>
0636             <AttributeName type="TextString" value="Name"/>
0637             <AttributeIndex type="Integer" value="1"/>
0638             <AttributeValue>
0639                 <NameValue type="TextString" value="TC-134-11-
certificate2"/>
0640                 <NameType type="Enumeration"
value="UninterpretedTextString"/>
0641             </AttributeValue>
0642         </Attribute>
0643     </ResponsePayload>
0644 </BatchItem>

```

0645	</ResponseMessage>
0646	# TIME 12
0647	<RequestMessage>
0648	<RequestHeader>
0649	<ProtocolVersion>
0650	<ProtocolVersionMajor type="Integer" value="1"/>
0651	<ProtocolVersionMinor type="Integer" value="1"/>
0652	</ProtocolVersion>
0653	<BatchCount type="Integer" value="1"/>
0654	</RequestHeader>
0655	<BatchItem>
0656	<Operation type="Enumeration" value="Destroy"/>
0657	<RequestPayload>
0658	<UniqueIdentifier type="TextString"
0659	value="\$UNIQUE_IDENTIFIER_1"/>
0660	</RequestPayload>
0661	</BatchItem>
0662	</RequestMessage>
0663	<ResponseMessage>
0664	<ResponseHeader>
0665	<ProtocolVersion>
0666	<ProtocolVersionMajor type="Integer" value="1"/>
0667	<ProtocolVersionMinor type="Integer" value="1"/>
0668	</ProtocolVersion>
0669	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0670	<BatchCount type="Integer" value="1"/>
0671	</ResponseHeader>
0672	<BatchItem>
0673	<Operation type="Enumeration" value="Destroy"/>
0674	<ResultStatus type="Enumeration" value="Success"/>
0675	<ResponsePayload>
0676	<UniqueIdentifier type="TextString"
0677	value="\$UNIQUE_IDENTIFIER_1"/>
0678	</ResponsePayload>
0679	</BatchItem>
0680	</ResponseMessage>
0681	# TIME 13
0682	<RequestMessage>
0683	<RequestHeader>
0684	<ProtocolVersion>
0685	<ProtocolVersionMajor type="Integer" value="1"/>
0686	<ProtocolVersionMinor type="Integer" value="1"/>
0687	</ProtocolVersion>
0688	<BatchCount type="Integer" value="1"/>
0689	</RequestHeader>
0690	<BatchItem>
0691	<Operation type="Enumeration" value="Destroy"/>
0692	<RequestPayload>
0693	<UniqueIdentifier type="TextString"
0694	value="\$UNIQUE_IDENTIFIER_0"/>
0695	</RequestPayload>
0696	</BatchItem>
0697	</RequestMessage>
0698	<ResponseMessage>
0699	<ResponseHeader>
0700	<ProtocolVersion>

0696	<ProtocolVersionMajor type="Integer" value="1"/>
0697	<ProtocolVersionMinor type="Integer" value="1"/>
0698	</ProtocolVersion>
0699	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0700	<BatchCount type="Integer" value="1"/>
0701	</ResponseHeader>
0702	<BatchItem>
0703	<Operation type="Enumeration" value="Destroy"/>
0704	<ResultStatus type="Enumeration" value="Success"/>
0705	<ResponsePayload>
0706	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0707	</ResponsePayload>
0708	</BatchItem>
0709	</ResponseMessage>
# TIME 14	
0710	<RequestMessage>
0711	<RequestHeader>
0712	<ProtocolVersion>
0713	<ProtocolVersionMajor type="Integer" value="1"/>
0714	<ProtocolVersionMinor type="Integer" value="1"/>
0715	</ProtocolVersion>
0716	<BatchCount type="Integer" value="1"/>
0717	</RequestHeader>
0718	<BatchItem>
0719	<Operation type="Enumeration" value="Destroy"/>
0720	<RequestPayload>
0721	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0722	</RequestPayload>
0723	</BatchItem>
0724	</RequestMessage>
0725	<ResponseMessage>
0726	<ResponseHeader>
0727	<ProtocolVersion>
0728	<ProtocolVersionMajor type="Integer" value="1"/>
0729	<ProtocolVersionMinor type="Integer" value="1"/>
0730	</ProtocolVersion>
0731	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0732	<BatchCount type="Integer" value="1"/>
0733	</ResponseHeader>
0734	<BatchItem>
0735	<Operation type="Enumeration" value="Destroy"/>
0736	<ResultStatus type="Enumeration" value="Success"/>
0737	<ResponsePayload>
0738	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0739	</ResponsePayload>
0740	</BatchItem>
0741	</ResponseMessage>
# TIME 15	
0742	<RequestMessage>
0743	<RequestHeader>
0744	<ProtocolVersion>
0745	<ProtocolVersionMajor type="Integer" value="1"/>
0746	<ProtocolVersionMinor type="Integer" value="1"/>

0747	</ProtocolVersion>
0748	<BatchCount type="Integer" value="1"/>
0749	</RequestHeader>
0750	<BatchItem>
0751	<Operation type="Enumeration" value="Destroy"/>
0752	<RequestPayload>
0753	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0754	</RequestPayload>
0755	</BatchItem>
0756	</RequestMessage>
0757	<ResponseMessage>
0758	<ResponseHeader>
0759	<ProtocolVersion>
0760	<ProtocolVersionMajor type="Integer" value="1"/>
0761	<ProtocolVersionMinor type="Integer" value="1"/>
0762	</ProtocolVersion>
0763	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0764	<BatchCount type="Integer" value="1"/>
0765	</ResponseHeader>
0766	<BatchItem>
0767	<Operation type="Enumeration" value="Destroy"/>
0768	<ResultStatus type="Enumeration" value="Success"/>
0769	<ResponsePayload>
0770	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0771	</ResponsePayload>
0772	</BatchItem>
0773	</ResponseMessage>

536

537 2.2.28 TC-141-11 - Key Wrapping using AES Key Wrap and No Encoding

538 Register a 128-bit AES key encryption key (KEK) with the Cryptographic Usage Mask attribute set
539 to Wrap and the Cryptographic Parameters specifying NIST Key Wrap as the Block Cipher Mode.
540 Subsequently, register another 128-bit AES data key (DEK). Retrieve the DEK wrapped using the
541 NIST Key Wrap algorithm and the KEK. The Cryptographic Usage Mask Attribute Name is
542 specified, indicating to the server that this attribute is to be wrapped together with the key
543 material. The Encoding Option field is omitted, which means that the default TTLV-encoding is
544 used. Finally, destroy both keys to return the server to the initial state.

545 The key material for both the KEK and the DEK are from the test vectors specified in Section 4.6
546 of [NISTKeyWrap].

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>

0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Name"/>
0016	<AttributeValue>
0017	<NameValue type="TextString" value="TC-141-11-key1"/>
0018	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0019	</AttributeValue>
0020	</Attribute>
0021	<Attribute>
0022	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0023	<AttributeValue type="Integer" value="WrapKey"/>
0024	</Attribute>
0025	<Attribute>
0026	<AttributeName type="TextString" value="Cryptographic
	Parameters"/>
0027	<AttributeValue>
0028	<BlockCipherMode type="Enumeration"
	value="NISTKeyWrap"/>
0029	</AttributeValue>
0030	</Attribute>
0031	<Attribute>
0032	<AttributeName type="TextString" value="Activation Date"/>
0033	<AttributeValue type="DateTime" value="\$NOW-3600"/>
0034	</Attribute>
0035	</TemplateAttribute>
0036	<SymmetricKey>
0037	<KeyBlock>
0038	<KeyFormatType type="Enumeration" value="Raw"/>
0039	<KeyValue>
0040	<KeyMaterial type="ByteString"
	value="000102030405060708090a0b0c0d0e0f"/>
0041	</KeyValue>
0042	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0043	<CryptographicLength type="Integer" value="128"/>
0044	</KeyBlock>
0045	</SymmetricKey>
0046	</RequestPayload>
0047	</BatchItem>
0048	</RequestMessage>
0049	<ResponseMessage>
0050	<ResponseHeader>
0051	<ProtocolVersion>
0052	<ProtocolVersionMajor type="Integer" value="1"/>
0053	<ProtocolVersionMinor type="Integer" value="1"/>
0054	</ProtocolVersion>
0055	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0056	<BatchCount type="Integer" value="1"/>
0057	</ResponseHeader>
0058	<BatchItem>
0059	<Operation type="Enumeration" value="Register"/>
0060	<ResultStatus type="Enumeration" value="Success"/>
0061	<ResponsePayload>

0062	<UniqueIdentifier type="TextString"
0063	value="\$UNIQUE_IDENTIFIER_0"/>
0064	</ResponsePayload>
0065	</BatchItem>
	</ResponseMessage>
	# TIME 1
0066	<RequestMessage>
0067	<RequestHeader>
0068	<ProtocolVersion>
0069	<ProtocolVersionMajor type="Integer" value="1"/>
0070	<ProtocolVersionMinor type="Integer" value="1"/>
0071	</ProtocolVersion>
0072	<BatchCount type="Integer" value="1"/>
0073	</RequestHeader>
0074	<BatchItem>
0075	<Operation type="Enumeration" value="Register"/>
0076	<RequestPayload>
0077	<ObjectType type="Enumeration" value="SymmetricKey"/>
0078	<TemplateAttribute>
0079	<Attribute>
0080	<AttributeName type="TextString" value="Name"/>
0081	<AttributeValue>
0082	<NameValue type="TextString" value="TC-141-11-key2"/>
0083	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0084	</AttributeValue>
0085	</Attribute>
0086	<Attribute>
0087	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0088	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0089	</Attribute>
0090	</TemplateAttribute>
0091	<SymmetricKey>
0092	<KeyBlock>
0093	<KeyFormatType type="Enumeration" value="Raw"/>
0094	<KeyValue>
0095	<KeyMaterial type="ByteString"
	value="00112233445566778899aabbccddeeff"/>
0096	</KeyValue>
0097	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0098	<CryptographicLength type="Integer" value="128"/>
0099	</KeyBlock>
0100	</SymmetricKey>
0101	</RequestPayload>
0102	</BatchItem>
0103	</RequestMessage>
0104	<ResponseMessage>
0105	<ResponseHeader>
0106	<ProtocolVersion>
0107	<ProtocolVersionMajor type="Integer" value="1"/>
0108	<ProtocolVersionMinor type="Integer" value="1"/>
0109	</ProtocolVersion>
0110	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0111	<BatchCount type="Integer" value="1"/>
0112	</ResponseHeader>
0113	<BatchItem>

0114	<Operation type="Enumeration" value="Register"/>
0115	<ResultStatus type="Enumeration" value="Success"/>
0116	<ResponsePayload>
0117	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0118	</ResponsePayload>
0119	</BatchItem>
0120	</ResponseMessage>
	# TIME 2
0121	<RequestMessage>
0122	<RequestHeader>
0123	<ProtocolVersion>
0124	<ProtocolVersionMajor type="Integer" value="1"/>
0125	<ProtocolVersionMinor type="Integer" value="1"/>
0126	</ProtocolVersion>
0127	<BatchCount type="Integer" value="1"/>
0128	</RequestHeader>
0129	<BatchItem>
0130	<Operation type="Enumeration" value="Get"/>
0131	<RequestPayload>
0132	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0133	<KeyWrappingSpecification>
0134	<WrappingMethod type="Enumeration" value="Encrypt"/>
0135	<EncryptionKeyInformation>
0136	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0137	<CryptographicParameters>
0138	<BlockCipherMode type="Enumeration"
	value="NISTKeyWrap"/>
0139	</CryptographicParameters>
0140	</EncryptionKeyInformation>
0141	<EncodingOption type="Enumeration" value="NoEncoding"/>
0142	</KeyWrappingSpecification>
0143	</RequestPayload>
0144	</BatchItem>
0145	</RequestMessage>
0146	<ResponseMessage>
0147	<ResponseHeader>
0148	<ProtocolVersion>
0149	<ProtocolVersionMajor type="Integer" value="1"/>
0150	<ProtocolVersionMinor type="Integer" value="1"/>
0151	</ProtocolVersion>
0152	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0153	<BatchCount type="Integer" value="1"/>
0154	</ResponseHeader>
0155	<BatchItem>
0156	<Operation type="Enumeration" value="Get"/>
0157	<ResultStatus type="Enumeration" value="Success"/>
0158	<ResponsePayload>
0159	<ObjectType type="Enumeration" value="SymmetricKey"/>
0160	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0161	<SymmetricKey>
0162	<KeyBlock>
0163	<KeyFormatType type="Enumeration" value="Raw"/>
0164	<KeyValue type="ByteString"

0165	value="1fa68b0a8112b447aef34bd8fb5a7b829d3e862371d2cfe5"/>
0166	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0167	<CryptographicLength type="Integer" value="128"/>
0168	<KeyWrappingData>
0169	<WrappingMethod type="Enumeration" value="Encrypt"/>
0170	<EncryptionKeyInformation>
0171	<UniqueIdentifier type="TextString"
0172	value="\$UNIQUE_IDENTIFIER_0"/>
0173	<CryptographicParameters>
0174	<BlockCipherMode type="Enumeration"
0175	value="NISTKeyWrap"/>
0176	</CryptographicParameters>
0177	</EncryptionKeyInformation>
0178	<EncodingOption type="Enumeration" value="NoEncoding"/>
0179	</KeyWrappingData>
0180	</KeyBlock>
0181	</SymmetricKey>
0182	</ResponsePayload>
0183	</BatchItem>
0184	</ResponseMessage>
0185	# TIME 3
0186	<RequestMessage>
0187	<RequestHeader>
0188	<ProtocolVersion>
0189	<ProtocolVersionMajor type="Integer" value="1"/>
0190	<ProtocolVersionMinor type="Integer" value="1"/>
0191	</ProtocolVersion>
0192	<BatchCount type="Integer" value="1"/>
0193	</RequestHeader>
0194	<BatchItem>
0195	<Operation type="Enumeration" value="Get"/>
0196	<RequestPayload>
0197	<UniqueIdentifier type="TextString"
0198	value="\$UNIQUE_IDENTIFIER_1"/>
0199	</RequestPayload>
0200	</BatchItem>
0201	</RequestMessage>
0202	<ResponseMessage>
0203	<ResponseHeader>
0204	<ProtocolVersion>
0205	<ProtocolVersionMajor type="Integer" value="1"/>
0206	<ProtocolVersionMinor type="Integer" value="1"/>
0207	</ProtocolVersion>
0208	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0209	<BatchCount type="Integer" value="1"/>
0210	</ResponseHeader>
0211	<BatchItem>
0212	<Operation type="Enumeration" value="Get"/>
0213	<ResultStatus type="Enumeration" value="Success"/>
0214	<ResponsePayload>
0215	<ObjectType type="Enumeration" value="SymmetricKey"/>
	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
	<SymmetricKey>
	<KeyBlock>
	<KeyFormatType type="Enumeration" value="Raw"/>
	<KeyValue>

0216	<KeyMaterial type="ByteString"
	value="00112233445566778899aabbccddeeff"/>
0217	</KeyValue>
0218	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0219	<CryptographicLength type="Integer" value="128"/>
0220	</KeyBlock>
0221	</SymmetricKey>
0222	</ResponsePayload>
0223	</BatchItem>
0224	</ResponseMessage>
	# TIME 4
0225	<RequestMessage>
0226	<RequestHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="1"/>
0230	</ProtocolVersion>
0231	<BatchCount type="Integer" value="1"/>
0232	</RequestHeader>
0233	<BatchItem>
0234	<Operation type="Enumeration" value="Destroy"/>
0235	<RequestPayload>
0236	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0237	</RequestPayload>
0238	</BatchItem>
0239	</RequestMessage>
0240	<ResponseMessage>
0241	<ResponseHeader>
0242	<ProtocolVersion>
0243	<ProtocolVersionMajor type="Integer" value="1"/>
0244	<ProtocolVersionMinor type="Integer" value="1"/>
0245	</ProtocolVersion>
0246	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0247	<BatchCount type="Integer" value="1"/>
0248	</ResponseHeader>
0249	<BatchItem>
0250	<Operation type="Enumeration" value="Destroy"/>
0251	<ResultStatus type="Enumeration" value="Success"/>
0252	<ResponsePayload>
0253	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0254	</ResponsePayload>
0255	</BatchItem>
0256	</ResponseMessage>
	# TIME 5
0257	<RequestMessage>
0258	<RequestHeader>
0259	<ProtocolVersion>
0260	<ProtocolVersionMajor type="Integer" value="1"/>
0261	<ProtocolVersionMinor type="Integer" value="2"/>
0262	</ProtocolVersion>
0263	<BatchCount type="Integer" value="1"/>
0264	</RequestHeader>
0265	<BatchItem>
0266	<Operation type="Enumeration" value="Revoke"/>

0267	<RequestPayload>
0268	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0269	<RevocationReason>
0270	<RevocationReasonCode type="Enumeration"
	value="Unspecified"/>
0271	</RevocationReason>
0272	</RequestPayload>
0273	</BatchItem>
0274	</RequestMessage>
0275	<ResponseMessage>
0276	<ResponseHeader>
0277	<ProtocolVersion>
0278	<ProtocolVersionMajor type="Integer" value="1"/>
0279	<ProtocolVersionMinor type="Integer" value="2"/>
0280	</ProtocolVersion>
0281	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0282	<BatchCount type="Integer" value="1"/>
0283	</ResponseHeader>
0284	<BatchItem>
0285	<Operation type="Enumeration" value="Revoke"/>
0286	<ResultStatus type="Enumeration" value="Success"/>
0287	<ResponsePayload>
0288	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0289	</ResponsePayload>
0290	</BatchItem>
0291	</ResponseMessage>
	# TIME 6
0292	<RequestMessage>
0293	<RequestHeader>
0294	<ProtocolVersion>
0295	<ProtocolVersionMajor type="Integer" value="1"/>
0296	<ProtocolVersionMinor type="Integer" value="1"/>
0297	</ProtocolVersion>
0298	<BatchCount type="Integer" value="1"/>
0299	</RequestHeader>
0300	<BatchItem>
0301	<Operation type="Enumeration" value="Destroy"/>
0302	<RequestPayload>
0303	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0304	</RequestPayload>
0305	</BatchItem>
0306	</RequestMessage>
0307	<ResponseMessage>
0308	<ResponseHeader>
0309	<ProtocolVersion>
0310	<ProtocolVersionMajor type="Integer" value="1"/>
0311	<ProtocolVersionMinor type="Integer" value="1"/>
0312	</ProtocolVersion>
0313	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0314	<BatchCount type="Integer" value="1"/>
0315	</ResponseHeader>
0316	<BatchItem>
0317	<Operation type="Enumeration" value="Destroy"/>

0318	<ResultStatus type="Enumeration" value="Success"/>
0319	<ResponsePayload>
0320	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0321	</ResponsePayload>
0322	</BatchItem>
0323	</ResponseMessage>

547

548 2.2.29 TC-142-11 - Key Wrapping using AES Key Wrap with Attributes

549 Register a 128-bit AES key encryption key (KEK) with the Cryptographic Usage Mask attribute set
550 to Wrap and the Cryptographic Parameters specifying NIST Key Wrap as the Block Cipher Mode.
551 Subsequently, register another 128-bit AES data key (DEK). Retrieve the data key wrapped using
552 the NIST Key Wrap algorithm and the KEK. The Encoding Option is set to No Encoding, which
553 means that only the key material is wrapped as opposed to the whole TTLV-encoded Key Value
554 structure being wrapped. Finally, destroy both keys to return the server to the initial state. The
555 key material for both the KEK and the DEK are from the test vectors specified in Section 4.6 of
556 [NISTKeyWrap].

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Name"/>
0016	<AttributeValue>
0017	<NameValue type="TextString" value="TC-142-11-key1"/>
0018	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0019	</AttributeValue>
0020	</Attribute>
0021	<Attribute>
0022	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0023	<AttributeValue type="Integer" value="WrapKey"/>
0024	</Attribute>
0025	<Attribute>
0026	<AttributeName type="TextString" value="Cryptographic
	Parameters"/>
0027	<AttributeValue>
0028	<BlockCipherMode type="Enumeration"
	value="NISTKeyWrap"/>
0029	</AttributeValue>

0030	</Attribute>
0031	<Attribute>
0032	<AttributeName type="TextString" value="Activation Date"/>
0033	<AttributeValue type="DateTime" value="\$NOW-3600"/>
0034	</Attribute>
0035	</TemplateAttribute>
0036	<SymmetricKey>
0037	<KeyBlock>
0038	<KeyFormatType type="Enumeration" value="Raw"/>
0039	<KeyValue>
0040	<KeyMaterial type="ByteString"
	value="000102030405060708090a0b0c0d0e0f"/>
0041	</KeyValue>
0042	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0043	<CryptographicLength type="Integer" value="128"/>
0044	</KeyBlock>
0045	</SymmetricKey>
0046	</RequestPayload>
0047	</BatchItem>
0048	</RequestMessage>
0049	<ResponseMessage>
0050	<ResponseHeader>
0051	<ProtocolVersion>
0052	<ProtocolVersionMajor type="Integer" value="1"/>
0053	<ProtocolVersionMinor type="Integer" value="1"/>
0054	</ProtocolVersion>
0055	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0056	<BatchCount type="Integer" value="1"/>
0057	</ResponseHeader>
0058	<BatchItem>
0059	<Operation type="Enumeration" value="Register"/>
0060	<ResultStatus type="Enumeration" value="Success"/>
0061	<ResponsePayload>
0062	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0063	</ResponsePayload>
0064	</BatchItem>
0065	</ResponseMessage>
	# TIME 1
0066	<RequestMessage>
0067	<RequestHeader>
0068	<ProtocolVersion>
0069	<ProtocolVersionMajor type="Integer" value="1"/>
0070	<ProtocolVersionMinor type="Integer" value="1"/>
0071	</ProtocolVersion>
0072	<BatchCount type="Integer" value="1"/>
0073	</RequestHeader>
0074	<BatchItem>
0075	<Operation type="Enumeration" value="Register"/>
0076	<RequestPayload>
0077	<ObjectType type="Enumeration" value="SymmetricKey"/>
0078	<TemplateAttribute>
0079	<Attribute>
0080	<AttributeName type="TextString" value="Name"/>
0081	<AttributeValue>
0082	<NameValue type="TextString" value="TC-142-11-key2"/>
0083	<NameType type="Enumeration"

0084	value="UninterpretedTextString"/>
0085	</AttributeValue>
0086	</Attribute>
0087	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0088	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0089	</Attribute>
0090	</TemplateAttribute>
0091	<SymmetricKey>
0092	<KeyBlock>
0093	<KeyFormatType type="Enumeration" value="Raw"/>
0094	<KeyValue>
0095	<KeyMaterial type="ByteString" value="00112233445566778899aabbccddeeff"/>
0096	</KeyValue>
0097	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0098	<CryptographicLength type="Integer" value="128"/>
0099	</KeyBlock>
0100	</SymmetricKey>
0101	</RequestPayload>
0102	</BatchItem>
0103	</RequestMessage>
0104	<ResponseMessage>
0105	<ResponseHeader>
0106	<ProtocolVersion>
0107	<ProtocolVersionMajor type="Integer" value="1"/>
0108	<ProtocolVersionMinor type="Integer" value="1"/>
0109	</ProtocolVersion>
0110	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0111	<BatchCount type="Integer" value="1"/>
0112	</ResponseHeader>
0113	<BatchItem>
0114	<Operation type="Enumeration" value="Register"/>
0115	<ResultStatus type="Enumeration" value="Success"/>
0116	<ResponsePayload>
0117	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0118	</ResponsePayload>
0119	</BatchItem>
0120	</ResponseMessage>
	# TIME 2
0121	<RequestMessage>
0122	<RequestHeader>
0123	<ProtocolVersion>
0124	<ProtocolVersionMajor type="Integer" value="1"/>
0125	<ProtocolVersionMinor type="Integer" value="1"/>
0126	</ProtocolVersion>
0127	<BatchCount type="Integer" value="1"/>
0128	</RequestHeader>
0129	<BatchItem>
0130	<Operation type="Enumeration" value="Get"/>
0131	<RequestPayload>
0132	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0133	<KeyWrappingSpecification>
0134	<WrappingMethod type="Enumeration" value="Encrypt"/>

0135	<EncryptionKeyInformation>
0136	<UniqueIdentifier type="TextString"
0137	value="\$UNIQUE_IDENTIFIER_0"/>
0138	<CryptographicParameters>
0139	<BlockCipherMode type="Enumeration"
0140	value="NISTKeyWrap"/>
0141	</CryptographicParameters>
0142	</EncryptionKeyInformation>
0143	<AttributeName type="TextString" value="Cryptographic Usage
0144	Mask"/>
0145	</KeyWrappingSpecification>
0146	</RequestPayload>
0147	</BatchItem>
0148	</RequestMessage>
0149	<ResponseMessage>
0150	<ResponseHeader>
0151	<ProtocolVersion>
0152	<ProtocolVersionMajor type="Integer" value="1"/>
0153	<ProtocolVersionMinor type="Integer" value="1"/>
0154	</ProtocolVersion>
0155	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0156	<BatchCount type="Integer" value="1"/>
0157	</ResponseHeader>
0158	<BatchItem>
0159	<Operation type="Enumeration" value="Get"/>
0160	<ResultStatus type="Enumeration" value="Success"/>
0161	<ResponsePayload>
0162	<ObjectType type="Enumeration" value="SymmetricKey"/>
0163	<UniqueIdentifier type="TextString"
0164	value="\$UNIQUE_IDENTIFIER_1"/>
0165	<SymmetricKey>
0166	<KeyBlock>
0167	<KeyFormatType type="Enumeration" value="Raw"/>
0168	<KeyValue type="ByteString"
0169	value="0dc0f8cb416e7b4422d85805d3dd80e49c6c75f763d1be99748de568e4eec
0170	dc05b94b1c1946fd3def14cfe184daada0daf07c93e038ceb9f501bdd8a82c7d6b33
0171	152dbf9d415924b9f13f6cb75ff880ab09dc862e473f74bdaf9398ec7695d41"/>
0172	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0173	<CryptographicLength type="Integer" value="128"/>
0174	<KeyWrappingData>
0175	<WrappingMethod type="Enumeration" value="Encrypt"/>
0176	<EncryptionKeyInformation>
0177	<UniqueIdentifier type="TextString"
0178	value="\$UNIQUE_IDENTIFIER_0"/>
0179	<CryptographicParameters>
0180	<BlockCipherMode type="Enumeration"
0181	value="NISTKeyWrap"/>
0182	</CryptographicParameters>
0183	</EncryptionKeyInformation>
0184	</KeyWrappingData>
0185	</KeyBlock>
0186	</SymmetricKey>
0187	</ResponsePayload>
0188	</BatchItem>
0189	</ResponseMessage>
0190	# TIME 3
0191	<RequestMessage>

0182	<RequestHeader>
0183	<ProtocolVersion>
0184	<ProtocolVersionMajor type="Integer" value="1"/>
0185	<ProtocolVersionMinor type="Integer" value="1"/>
0186	</ProtocolVersion>
0187	<BatchCount type="Integer" value="1"/>
0188	</RequestHeader>
0189	<BatchItem>
0190	<Operation type="Enumeration" value="Get"/>
0191	<RequestPayload>
0192	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0193	</RequestPayload>
0194	</BatchItem>
0195	</RequestMessage>
0196	<ResponseMessage>
0197	<ResponseHeader>
0198	<ProtocolVersion>
0199	<ProtocolVersionMajor type="Integer" value="1"/>
0200	<ProtocolVersionMinor type="Integer" value="1"/>
0201	</ProtocolVersion>
0202	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0203	<BatchCount type="Integer" value="1"/>
0204	</ResponseHeader>
0205	<BatchItem>
0206	<Operation type="Enumeration" value="Get"/>
0207	<ResultStatus type="Enumeration" value="Success"/>
0208	<ResponsePayload>
0209	<ObjectType type="Enumeration" value="SymmetricKey"/>
0210	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0211	<SymmetricKey>
0212	<KeyBlock>
0213	<KeyFormatType type="Enumeration" value="Raw"/>
0214	<KeyValue>
0215	<KeyMaterial type="ByteString"
	value="00112233445566778899aabbccddeeff"/>
0216	</KeyValue>
0217	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0218	<CryptographicLength type="Integer" value="128"/>
0219	</KeyBlock>
0220	</SymmetricKey>
0221	</ResponsePayload>
0222	</BatchItem>
0223	</ResponseMessage>
	# TIME 4
0224	<RequestMessage>
0225	<RequestHeader>
0226	<ProtocolVersion>
0227	<ProtocolVersionMajor type="Integer" value="1"/>
0228	<ProtocolVersionMinor type="Integer" value="1"/>
0229	</ProtocolVersion>
0230	<BatchCount type="Integer" value="1"/>
0231	</RequestHeader>
0232	<BatchItem>
0233	<Operation type="Enumeration" value="Destroy"/>
0234	<RequestPayload>

0235	<UniqueIdentifier type="TextString"
0236	value="\$UNIQUE_IDENTIFIER_1"/>
0237	</RequestPayload>
0238	</BatchItem>
0239	</RequestMessage>
0239	<ResponseMessage>
0240	<ResponseHeader>
0241	<ProtocolVersion>
0242	<ProtocolVersionMajor type="Integer" value="1"/>
0243	<ProtocolVersionMinor type="Integer" value="1"/>
0244	</ProtocolVersion>
0245	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0246	<BatchCount type="Integer" value="1"/>
0247	</ResponseHeader>
0248	<BatchItem>
0249	<Operation type="Enumeration" value="Destroy"/>
0250	<ResultStatus type="Enumeration" value="Success"/>
0251	<ResponsePayload>
0252	<UniqueIdentifier type="TextString"
0253	value="\$UNIQUE_IDENTIFIER_1"/>
0254	</ResponsePayload>
0255	</BatchItem>
0256	</ResponseMessage>
0256	# TIME 5
0257	<RequestMessage>
0258	<RequestHeader>
0259	<ProtocolVersion>
0260	<ProtocolVersionMajor type="Integer" value="1"/>
0261	<ProtocolVersionMinor type="Integer" value="2"/>
0262	</ProtocolVersion>
0263	<BatchCount type="Integer" value="1"/>
0264	</RequestHeader>
0265	<BatchItem>
0266	<Operation type="Enumeration" value="Revoke"/>
0267	<RequestPayload>
0268	<UniqueIdentifier type="TextString"
0269	value="\$UNIQUE_IDENTIFIER_0"/>
0270	<RevocationReason>
0271	<RevocationReasonCode type="Enumeration"
0272	value="Unspecified"/>
0273	</RevocationReason>
0274	</RequestPayload>
0275	</BatchItem>
0276	</RequestMessage>
0274	<ResponseMessage>
0275	<ResponseHeader>
0276	<ProtocolVersion>
0277	<ProtocolVersionMajor type="Integer" value="1"/>
0278	<ProtocolVersionMinor type="Integer" value="2"/>
0279	</ProtocolVersion>
0280	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0281	<BatchCount type="Integer" value="1"/>
0282	</ResponseHeader>
0283	<BatchItem>
0284	<Operation type="Enumeration" value="Revoke"/>
0285	<ResultStatus type="Enumeration" value="Success"/>

0286	<ResponsePayload>
0287	<UniqueIdentifier type="TextString"
0288	value="\$UNIQUE_IDENTIFIER_0"/>
0289	</ResponsePayload>
0290	</BatchItem>
0291	</ResponseMessage>
0291	# TIME 6
0291	<RequestMessage>
0292	<RequestHeader>
0293	<ProtocolVersion>
0294	<ProtocolVersionMajor type="Integer" value="1"/>
0295	<ProtocolVersionMinor type="Integer" value="1"/>
0296	</ProtocolVersion>
0297	<BatchCount type="Integer" value="1"/>
0298	</RequestHeader>
0299	<BatchItem>
0300	<Operation type="Enumeration" value="Destroy"/>
0301	<RequestPayload>
0302	<UniqueIdentifier type="TextString"
0303	value="\$UNIQUE_IDENTIFIER_0"/>
0304	</RequestPayload>
0305	</BatchItem>
0306	</RequestMessage>
0306	<ResponseMessage>
0307	<ResponseHeader>
0308	<ProtocolVersion>
0309	<ProtocolVersionMajor type="Integer" value="1"/>
0310	<ProtocolVersionMinor type="Integer" value="1"/>
0311	</ProtocolVersion>
0312	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0313	<BatchCount type="Integer" value="1"/>
0314	</ResponseHeader>
0315	<BatchItem>
0316	<Operation type="Enumeration" value="Destroy"/>
0317	<ResultStatus type="Enumeration" value="Success"/>
0318	<ResponsePayload>
0319	<UniqueIdentifier type="TextString"
0320	value="\$UNIQUE_IDENTIFIER_0"/>
0321	</ResponsePayload>
0322	</BatchItem>
0322	</ResponseMessage>

557

558 2.2.30 TC-151-11 - Locate a Fresh Object from the Default Group

559 Locate a single fresh object from the default object group. Perform a Get Attribute to retrieve
560 the value of the Fresh attribute to make sure that the key is fresh. Get the object (the kind of
561 object returned depends on the server policy), and get the Fresh attribute again to verify that
562 the object is no longer fresh. Finally, destroy the object. This test case illustrates only one
563 possible behavior related to the default group. In this test case, it is assumed that the server has
564 fresh objects available in the default group, or that it creates a new object on-the-fly as a
565 consequence of the Locate request. It is also assumed that no other client retrieves the object
566 after the Locate but before the batched Get Attributes request, thereby toggling the value of the
567 Fresh attribute.

	# TIME 0
0001	<RequestMessage> <RequestHeader>
0002	<ProtocolVersion>
0003	<ProtocolVersionMajor type="Integer" value="1"/>
0004	<ProtocolVersionMinor type="Integer" value="1"/>
0005	</ProtocolVersion>
0006	<BatchOrderOption type="Boolean" value="true"/>
0007	<BatchCount type="Integer" value="2"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Locate"/>
0011	<UniqueBatchItemID type="ByteString" value="1e766d8a95d6e5d1"/>
0012	<RequestPayload>
0013	<MaximumItems type="Integer" value="1"/>
0014	<ObjectGroupMember type="Enumeration"
0015	value="GroupMemberFresh"/>
0016	<Attribute>
0017	<AttributeName type="TextString" value="Object Group"/>
0018	<AttributeValue type="TextString" value="default"/>
0019	</Attribute>
0020	</RequestPayload>
0021	</BatchItem>
0022	<BatchItem>
0023	<Operation type="Enumeration" value="GetAttributes"/>
0024	<UniqueBatchItemID type="ByteString" value="8650f83be5373722"/>
0025	<RequestPayload>
0026	<AttributeName type="TextString" value="Fresh"/>
0027	</RequestPayload>
0028	</BatchItem>
0029	</RequestMessage>
0030	<ResponseMessage>
0031	<ResponseHeader>
0032	<ProtocolVersion>
0033	<ProtocolVersionMajor type="Integer" value="1"/>
0034	<ProtocolVersionMinor type="Integer" value="1"/>
0035	</ProtocolVersion>
0036	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0037	<BatchCount type="Integer" value="2"/>
0038	</ResponseHeader>
0039	<BatchItem>
0040	<Operation type="Enumeration" value="Locate"/>
0041	<UniqueBatchItemID type="ByteString" value="1e766d8a95d6e5d1"/>
0042	<ResultStatus type="Enumeration" value="Success"/>
0043	<ResponsePayload>
0044	<UniqueIdentifier type="TextString"
0045	value="\$UNIQUE_IDENTIFIER_0"/>
0046	</ResponsePayload>
0047	</BatchItem>
0048	<BatchItem>
0049	<Operation type="Enumeration" value="GetAttributes"/>
0050	<UniqueBatchItemID type="ByteString" value="8650f83be5373722"/>
0051	<ResultStatus type="Enumeration" value="Success"/>
0052	<ResponsePayload>
0053	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
	<Attribute>
	<AttributeName type="TextString" value="Fresh"/>

0054	<AttributeValue type="Boolean" value="true"/>
0055	</Attribute>
0056	</ResponsePayload>
0057	</BatchItem>
0058	</ResponseMessage>
# TIME 1	
0059	<RequestMessage>
0060	<RequestHeader>
0061	<ProtocolVersion>
0062	<ProtocolVersionMajor type="Integer" value="1"/>
0063	<ProtocolVersionMinor type="Integer" value="1"/>
0064	</ProtocolVersion>
0065	<BatchCount type="Integer" value="1"/>
0066	</RequestHeader>
0067	<BatchItem>
0068	<Operation type="Enumeration" value="Get"/>
0069	<RequestPayload>
0070	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0071	</RequestPayload>
0072	</BatchItem>
0073	</RequestMessage>
0074	<ResponseMessage>
0075	<ResponseHeader>
0076	<ProtocolVersion>
0077	<ProtocolVersionMajor type="Integer" value="1"/>
0078	<ProtocolVersionMinor type="Integer" value="1"/>
0079	</ProtocolVersion>
0080	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0081	<BatchCount type="Integer" value="1"/>
0082	</ResponseHeader>
0083	<BatchItem>
0084	<Operation type="Enumeration" value="Get"/>
0085	<ResultStatus type="Enumeration" value="Success"/>
0086	<ResponsePayload>
0087	<ObjectType type="Enumeration" value="SymmetricKey"/>
0088	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0089	<SymmetricKey>
0090	<KeyBlock>
0091	<KeyFormatType type="Enumeration" value="Raw"/>
0092	<KeyValue>
0093	<KeyMaterial type="ByteString"
	value="7fe09d434868ae14a0021ac19330f8d9226790d680e519f8ac25f42d72f60f0c"/>
0094	</KeyValue>
0095	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0096	<CryptographicLength type="Integer" value="256"/>
0097	</KeyBlock>
0098	</SymmetricKey>
0099	</ResponsePayload>
0100	</BatchItem>
0101	</ResponseMessage>
# TIME 2	
0102	<RequestMessage>
0103	<RequestHeader>

0104	<ProtocolVersion>
0105	<ProtocolVersionMajor type="Integer" value="1"/>
0106	<ProtocolVersionMinor type="Integer" value="1"/>
0107	</ProtocolVersion>
0108	<BatchCount type="Integer" value="1"/>
0109	</RequestHeader>
0110	<BatchItem>
0111	<Operation type="Enumeration" value="GetAttributes"/>
0112	<RequestPayload>
0113	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0114	<AttributeName type="TextString" value="Fresh"/>
0115	</RequestPayload>
0116	</BatchItem>
0117	</RequestMessage>
0118	<ResponseMessage>
0119	<ResponseHeader>
0120	<ProtocolVersion>
0121	<ProtocolVersionMajor type="Integer" value="1"/>
0122	<ProtocolVersionMinor type="Integer" value="1"/>
0123	</ProtocolVersion>
0124	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0125	<BatchCount type="Integer" value="1"/>
0126	</ResponseHeader>
0127	<BatchItem>
0128	<Operation type="Enumeration" value="GetAttributes"/>
0129	<ResultStatus type="Enumeration" value="Success"/>
0130	<ResponsePayload>
0131	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0132	<Attribute>
0133	<AttributeName type="TextString" value="Fresh"/>
0134	<AttributeValue type="Boolean" value="false"/>
0135	</Attribute>
0136	</ResponsePayload>
0137	</BatchItem>
0138	</ResponseMessage>
	# TIME 3
0139	<RequestMessage>
0140	<RequestHeader>
0141	<ProtocolVersion>
0142	<ProtocolVersionMajor type="Integer" value="1"/>
0143	<ProtocolVersionMinor type="Integer" value="1"/>
0144	</ProtocolVersion>
0145	<BatchCount type="Integer" value="1"/>
0146	</RequestHeader>
0147	<BatchItem>
0148	<Operation type="Enumeration" value="Destroy"/>
0149	<RequestPayload>
0150	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0151	</RequestPayload>
0152	</BatchItem>
0153	</RequestMessage>
0154	<ResponseMessage>
0155	<ResponseHeader>

```

0156     <ProtocolVersion>
0157         <ProtocolVersionMajor type="Integer" value="1"/>
0158         <ProtocolVersionMinor type="Integer" value="1"/>
0159     </ProtocolVersion>
0160     <TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0161     <BatchCount type="Integer" value="1"/>
0162 </ResponseHeader>
0163 <BatchItem>
0164     <Operation type="Enumeration" value="Destroy"/>
0165     <ResultStatus type="Enumeration" value="Success"/>
0166     <ResponsePayload>
0167         <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0168     </ResponsePayload>
0169 </BatchItem>
0170 </ResponseMessage>

```

568

569 2.2.31 TC-152-11 - Client-side Group Management

570 Register two symmetric keys, both with the same (non-default) Object Group name specified
571 and the Fresh attribute set to true. Get the Fresh attribute from both keys to make sure it was
572 set. Perform three batched Locate and Get requests to get a fresh key from the group. The first
573 two requests should return both the registered keys, whereas the third request should return no
574 key. To clean up, destroy both keys. This test case assumes that the server supports and sets
575 the Fresh attribute when requested to do so by the client.

```

# TIME 0
0001 <RequestMessage>
0002     <RequestHeader>
0003         <ProtocolVersion>
0004             <ProtocolVersionMajor type="Integer" value="1"/>
0005             <ProtocolVersionMinor type="Integer" value="1"/>
0006         </ProtocolVersion>
0007         <BatchCount type="Integer" value="1"/>
0008     </RequestHeader>
0009     <BatchItem>
0010         <Operation type="Enumeration" value="Register"/>
0011         <RequestPayload>
0012             <ObjectType type="Enumeration" value="SymmetricKey"/>
0013             <TemplateAttribute>
0014                 <Attribute>
0015                     <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0016                     <AttributeValue type="Enumeration" value="AES"/>
0017                 </Attribute>
0018                 <Attribute>
0019                     <AttributeName type="TextString" value="Cryptographic
Length"/>
0020                     <AttributeValue type="Integer" value="256"/>
0021                 </Attribute>
0022                 <Attribute>
0023                     <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0024                     <AttributeValue type="Integer" value="Decrypt Encrypt"/>

```


0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Object Group"/>
0028	<AttributeValue type="TextString"
	value="ClientFreshTest"/>
0029	</Attribute>
0030	<Attribute>
0031	<AttributeName type="TextString" value="Fresh"/>
0032	<AttributeValue type="Boolean" value="true"/>
0033	</Attribute>
0034	<Attribute>
0035	<AttributeName type="TextString" value="x-ID"/>
0036	<AttributeValue type="TextString" value="TC-152-11-key1"/>
0037	</Attribute>
0038	</TemplateAttribute>
0039	<SymmetricKey>
0040	<KeyBlock>
0041	<KeyFormatType type="Enumeration" value="Raw"/>
0042	<KeyValue>
0043	<KeyMaterial type="ByteString"
	value="000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1elf"/>
0044	</KeyValue>
0045	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0046	<CryptographicLength type="Integer" value="256"/>
0047	</KeyBlock>
0048	</SymmetricKey>
0049	</RequestPayload>
0050	</BatchItem>
0051	</RequestMessage>
0052	<ResponseMessage>
0053	<ResponseHeader>
0054	<ProtocolVersion>
0055	<ProtocolVersionMajor type="Integer" value="1"/>
0056	<ProtocolVersionMinor type="Integer" value="1"/>
0057	</ProtocolVersion>
0058	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0059	<BatchCount type="Integer" value="1"/>
0060	</ResponseHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<ResultStatus type="Enumeration" value="Success"/>
0064	<ResponsePayload>
0065	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
	# TIME 1
0069	<RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="1"/>
0074	</ProtocolVersion>
0075	<BatchCount type="Integer" value="1"/>
0076	</RequestHeader>

0077	<BatchItem>
0078	<Operation type="Enumeration" value="Register"/>
0079	<RequestPayload>
0080	<ObjectType type="Enumeration" value="SymmetricKey"/>
0081	<TemplateAttribute>
0082	<Attribute>
0083	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0084	<AttributeValue type="Enumeration" value="AES"/>
0085	</Attribute>
0086	<Attribute>
0087	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0088	<AttributeValue type="Integer" value="256"/>
0089	</Attribute>
0090	<Attribute>
0091	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0092	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0093	</Attribute>
0094	<Attribute>
0095	<AttributeName type="TextString" value="Object Group"/>
0096	<AttributeValue type="TextString"
	value="ClientFreshTest"/>
0097	</Attribute>
0098	<Attribute>
0099	<AttributeName type="TextString" value="Fresh"/>
0100	<AttributeValue type="Boolean" value="true"/>
0101	</Attribute>
0102	<Attribute>
0103	<AttributeName type="TextString" value="x-ID"/>
0104	<AttributeValue type="TextString" value="TC-152-11-key2"/>
0105	</Attribute>
0106	</TemplateAttribute>
0107	<SymmetricKey>
0108	<KeyBlock>
0109	<KeyFormatType type="Enumeration" value="Raw"/>
0110	<KeyValue>
0111	<KeyMaterial type="ByteString"
	value="00112233445566778899aabbccddeeff000102030405060708090a0b0c0d0
	e0f"/>
0112	</KeyValue>
0113	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0114	<CryptographicLength type="Integer" value="256"/>
0115	</KeyBlock>
0116	</SymmetricKey>
0117	</RequestPayload>
0118	</BatchItem>
0119	</RequestMessage>
0120	<ResponseMessage>
0121	<ResponseHeader>
0122	<ProtocolVersion>
0123	<ProtocolVersionMajor type="Integer" value="1"/>
0124	<ProtocolVersionMinor type="Integer" value="1"/>
0125	</ProtocolVersion>
0126	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0127	<BatchCount type="Integer" value="1"/>

0128	</ResponseHeader>
0129	<BatchItem>
0130	<Operation type="Enumeration" value="Register"/>
0131	<ResultStatus type="Enumeration" value="Success"/>
0132	<ResponsePayload>
0133	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0134	</ResponsePayload>
0135	</BatchItem>
0136	</ResponseMessage>
# TIME 2	
0137	<RequestMessage>
0138	<RequestHeader>
0139	<ProtocolVersion>
0140	<ProtocolVersionMajor type="Integer" value="1"/>
0141	<ProtocolVersionMinor type="Integer" value="1"/>
0142	</ProtocolVersion>
0143	<BatchCount type="Integer" value="1"/>
0144	</RequestHeader>
0145	<BatchItem>
0146	<Operation type="Enumeration" value="GetAttributes"/>
0147	<RequestPayload>
0148	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0149	<AttributeName type="TextString" value="Fresh"/>
0150	</RequestPayload>
0151	</BatchItem>
0152	</RequestMessage>
0153	<ResponseMessage>
0154	<ResponseHeader>
0155	<ProtocolVersion>
0156	<ProtocolVersionMajor type="Integer" value="1"/>
0157	<ProtocolVersionMinor type="Integer" value="1"/>
0158	</ProtocolVersion>
0159	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0160	<BatchCount type="Integer" value="1"/>
0161	</ResponseHeader>
0162	<BatchItem>
0163	<Operation type="Enumeration" value="GetAttributes"/>
0164	<ResultStatus type="Enumeration" value="Success"/>
0165	<ResponsePayload>
0166	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0167	<Attribute>
0168	<AttributeName type="TextString" value="Fresh"/>
0169	<AttributeValue type="Boolean" value="true"/>
0170	</Attribute>
0171	</ResponsePayload>
0172	</BatchItem>
0173	</ResponseMessage>
# TIME 3	
0174	<RequestMessage>
0175	<RequestHeader>
0176	<ProtocolVersion>
0177	<ProtocolVersionMajor type="Integer" value="1"/>
0178	<ProtocolVersionMinor type="Integer" value="1"/>

0179	</ProtocolVersion>
0180	<BatchCount type="Integer" value="1"/>
0181	</RequestHeader>
0182	<BatchItem>
0183	<Operation type="Enumeration" value="GetAttributes"/>
0184	<RequestPayload>
0185	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0186	<AttributeName type="TextString" value="Fresh"/>
0187	</RequestPayload>
0188	</BatchItem>
0189	</RequestMessage>
0190	<ResponseMessage>
0191	<ResponseHeader>
0192	<ProtocolVersion>
0193	<ProtocolVersionMajor type="Integer" value="1"/>
0194	<ProtocolVersionMinor type="Integer" value="1"/>
0195	</ProtocolVersion>
0196	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0197	<BatchCount type="Integer" value="1"/>
0198	</ResponseHeader>
0199	<BatchItem>
0200	<Operation type="Enumeration" value="GetAttributes"/>
0201	<ResultStatus type="Enumeration" value="Success"/>
0202	<ResponsePayload>
0203	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0204	<Attribute>
0205	<AttributeName type="TextString" value="Fresh"/>
0206	<AttributeValue type="Boolean" value="true"/>
0207	</Attribute>
0208	</ResponsePayload>
0209	</BatchItem>
0210	</ResponseMessage>
	# TIME 4
0211	<RequestMessage>
0212	<RequestHeader>
0213	<ProtocolVersion>
0214	<ProtocolVersionMajor type="Integer" value="1"/>
0215	<ProtocolVersionMinor type="Integer" value="1"/>
0216	</ProtocolVersion>
0217	<BatchOrderOption type="Boolean" value="true"/>
0218	<BatchCount type="Integer" value="2"/>
0219	</RequestHeader>
0220	<BatchItem>
0221	<Operation type="Enumeration" value="Locate"/>
0222	<UniqueBatchItemID type="ByteString" value="294fb5e3e93f8ecc"/>
0223	<RequestPayload>
0224	<MaximumItems type="Integer" value="1"/>
0225	<ObjectGroupMember type="Enumeration"
	value="GroupMemberFresh"/>
0226	<Attribute>
0227	<AttributeName type="TextString" value="Object Group"/>
0228	<AttributeValue type="TextString" value="ClientFreshTest"/>
0229	</Attribute>
0230	</RequestPayload>
0231	</BatchItem>

0232	<BatchItem>
0233	<Operation type="Enumeration" value="Get"/>
0234	<UniqueBatchItemID type="ByteString" value="9da79a935d4e4ae6"/>
0235	<RequestPayload>
0236	</RequestPayload>
0237	</BatchItem>
0238	</RequestMessage>
0239	<ResponseMessage>
0240	<ResponseHeader>
0241	<ProtocolVersion>
0242	<ProtocolVersionMajor type="Integer" value="1"/>
0243	<ProtocolVersionMinor type="Integer" value="1"/>
0244	</ProtocolVersion>
0245	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0246	<BatchCount type="Integer" value="2"/>
0247	</ResponseHeader>
0248	<BatchItem>
0249	<Operation type="Enumeration" value="Locate"/>
0250	<UniqueBatchItemID type="ByteString" value="294fb5e3e93f8ecc"/>
0251	<ResultStatus type="Enumeration" value="Success"/>
0252	<ResponsePayload>
0253	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0254	</ResponsePayload>
0255	</BatchItem>
0256	<BatchItem>
0257	<Operation type="Enumeration" value="Get"/>
0258	<UniqueBatchItemID type="ByteString" value="9da79a935d4e4ae6"/>
0259	<ResultStatus type="Enumeration" value="Success"/>
0260	<ResponsePayload>
0261	<ObjectType type="Enumeration" value="SymmetricKey"/>
0262	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0263	<SymmetricKey>
0264	<KeyBlock>
0265	<KeyFormatType type="Enumeration" value="Raw"/>
0266	<KeyValue>
0267	<KeyMaterial type="ByteString"
	value="000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1elf"/>
0268	</KeyValue>
0269	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0270	<CryptographicLength type="Integer" value="256"/>
0271	</KeyBlock>
0272	</SymmetricKey>
0273	</ResponsePayload>
0274	</BatchItem>
0275	</ResponseMessage>
	# TIME 5
0276	<RequestMessage>
0277	<RequestHeader>
0278	<ProtocolVersion>
0279	<ProtocolVersionMajor type="Integer" value="1"/>
0280	<ProtocolVersionMinor type="Integer" value="1"/>
0281	</ProtocolVersion>
0282	<BatchOrderOption type="Boolean" value="true"/>
0283	<BatchCount type="Integer" value="2"/>

0284	</RequestHeader>
0285	<BatchItem>
0286	<Operation type="Enumeration" value="Locate"/>
0287	<UniqueBatchItemID type="ByteString" value="85e3e21d14d6df1d"/>
0288	<RequestPayload>
0289	<MaximumItems type="Integer" value="1"/>
0290	<ObjectGroupMember type="Enumeration"
	value="GroupMemberFresh"/>
0291	<Attribute>
0292	<AttributeName type="TextString" value="Object Group"/>
0293	<AttributeValue type="TextString" value="ClientFreshTest"/>
0294	</Attribute>
0295	</RequestPayload>
0296	</BatchItem>
0297	<BatchItem>
0298	<Operation type="Enumeration" value="Get"/>
0299	<UniqueBatchItemID type="ByteString" value="40feae5ec1bda875"/>
0300	<RequestPayload>
0301	</RequestPayload>
0302	</BatchItem>
0303	</RequestMessage>
0304	<ResponseMessage>
0305	<ResponseHeader>
0306	<ProtocolVersion>
0307	<ProtocolVersionMajor type="Integer" value="1"/>
0308	<ProtocolVersionMinor type="Integer" value="1"/>
0309	</ProtocolVersion>
0310	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0311	<BatchCount type="Integer" value="2"/>
0312	</ResponseHeader>
0313	<BatchItem>
0314	<Operation type="Enumeration" value="Locate"/>
0315	<UniqueBatchItemID type="ByteString" value="85e3e21d14d6df1d"/>
0316	<ResultStatus type="Enumeration" value="Success"/>
0317	<ResponsePayload>
0318	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0319	</ResponsePayload>
0320	</BatchItem>
0321	<BatchItem>
0322	<Operation type="Enumeration" value="Get"/>
0323	<UniqueBatchItemID type="ByteString" value="40feae5ec1bda875"/>
0324	<ResultStatus type="Enumeration" value="Success"/>
0325	<ResponsePayload>
0326	<ObjectType type="Enumeration" value="SymmetricKey"/>
0327	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0328	<SymmetricKey>
0329	<KeyBlock>
0330	<KeyFormatType type="Enumeration" value="Raw"/>
0331	<KeyValue>
0332	<KeyMaterial type="ByteString"
	value="00112233445566778899aabbccddeeff000102030405060708090a0b0c0d0e0f"/>
0333	</KeyValue>
0334	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0335	<CryptographicLength type="Integer" value="256"/>

0336	</KeyBlock>
0337	</SymmetricKey>
0338	</ResponsePayload>
0339	</BatchItem>
0340	</ResponseMessage>
# TIME 6	
0341	<RequestMessage>
0342	<RequestHeader>
0343	<ProtocolVersion>
0344	<ProtocolVersionMajor type="Integer" value="1"/>
0345	<ProtocolVersionMinor type="Integer" value="1"/>
0346	</ProtocolVersion>
0347	<BatchOrderOption type="Boolean" value="true"/>
0348	<BatchCount type="Integer" value="2"/>
0349	</RequestHeader>
0350	<BatchItem>
0351	<Operation type="Enumeration" value="Locate"/>
0352	<UniqueBatchItemID type="ByteString" value="657339bdf375bfa2"/>
0353	<RequestPayload>
0354	<MaximumItems type="Integer" value="1"/>
0355	<ObjectGroupMember type="Enumeration"
0356	value="GroupMemberFresh"/>
0357	<Attribute>
0358	<AttributeName type="TextString" value="Object Group"/>
0359	<AttributeValue type="TextString" value="ClientFreshTest"/>
0360	</Attribute>
0361	</RequestPayload>
0362	</BatchItem>
0363	<BatchItem>
0364	<Operation type="Enumeration" value="Get"/>
0365	<UniqueBatchItemID type="ByteString" value="5713c4911444b36e"/>
0366	<RequestPayload>
0367	</RequestPayload>
0368	</BatchItem>
0369	</RequestMessage>
0370	<ResponseMessage>
0371	<ResponseHeader>
0372	<ProtocolVersion>
0373	<ProtocolVersionMajor type="Integer" value="1"/>
0374	<ProtocolVersionMinor type="Integer" value="1"/>
0375	</ProtocolVersion>
0376	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0377	<BatchCount type="Integer" value="2"/>
0378	</ResponseHeader>
0379	<BatchItem>
0380	<Operation type="Enumeration" value="Locate"/>
0381	<UniqueBatchItemID type="ByteString" value="657339bdf375bfa2"/>
0382	<ResultStatus type="Enumeration" value="Success"/>
0383	<ResponsePayload>
0384	</ResponsePayload>
0385	</BatchItem>
0386	<BatchItem>
0387	<Operation type="Enumeration" value="Get"/>
0388	<UniqueBatchItemID type="ByteString" value="5713c4911444b36e"/>
0389	<ResultStatus type="Enumeration" value="OperationFailed"/>
0390	<ResultReason type="Enumeration" value="ItemNotFound"/>
0391	<ResultMessage type="TextString" value="NOT FOUND"/>

0391	</BatchItem>
0392	</ResponseMessage>
# TIME 7	
0393	<RequestMessage>
0394	<RequestHeader>
0395	<ProtocolVersion>
0396	<ProtocolVersionMajor type="Integer" value="1"/>
0397	<ProtocolVersionMinor type="Integer" value="1"/>
0398	</ProtocolVersion>
0399	<BatchCount type="Integer" value="1"/>
0400	</RequestHeader>
0401	<BatchItem>
0402	<Operation type="Enumeration" value="Destroy"/>
0403	<RequestPayload>
0404	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0405	</RequestPayload>
0406	</BatchItem>
0407	</RequestMessage>
0408	<ResponseMessage>
0409	<ResponseHeader>
0410	<ProtocolVersion>
0411	<ProtocolVersionMajor type="Integer" value="1"/>
0412	<ProtocolVersionMinor type="Integer" value="1"/>
0413	</ProtocolVersion>
0414	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0415	<BatchCount type="Integer" value="1"/>
0416	</ResponseHeader>
0417	<BatchItem>
0418	<Operation type="Enumeration" value="Destroy"/>
0419	<ResultStatus type="Enumeration" value="Success"/>
0420	<ResponsePayload>
0421	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0422	</ResponsePayload>
0423	</BatchItem>
0424	</ResponseMessage>
# TIME 8	
0425	<RequestMessage>
0426	<RequestHeader>
0427	<ProtocolVersion>
0428	<ProtocolVersionMajor type="Integer" value="1"/>
0429	<ProtocolVersionMinor type="Integer" value="1"/>
0430	</ProtocolVersion>
0431	<BatchCount type="Integer" value="1"/>
0432	</RequestHeader>
0433	<BatchItem>
0434	<Operation type="Enumeration" value="Destroy"/>
0435	<RequestPayload>
0436	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0437	</RequestPayload>
0438	</BatchItem>
0439	</RequestMessage>
0440	<ResponseMessage>
0441	<ResponseHeader>


```
0442 <ProtocolVersion>
0443   <ProtocolVersionMajor type="Integer" value="1"/>
0444   <ProtocolVersionMinor type="Integer" value="1"/>
0445 </ProtocolVersion>
0446 <TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0447 <BatchCount type="Integer" value="1"/>
0448 </ResponseHeader>
0449 <BatchItem>
0450   <Operation type="Enumeration" value="Destroy"/>
0451   <ResultStatus type="Enumeration" value="Success"/>
0452   <ResponsePayload>
0453     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0454   </ResponsePayload>
0455 </BatchItem>
0456 </ResponseMessage>
```

576

577 2.2.32 TC-153-11 - Default Object Group Member

578 This test case exercises the 'default' Object Group Member flag in the Locate request. Three
579 keys are created on the server and put into the same group (the Object Group attribute is set to
580 the same value for all keys). Thereafter, the client performs four batched Locate and Get
581 requests, asking for the default object from the group. This test case assumes that the server
582 policy is such that it serves objects from the group in a round-robin fashion. The pointer to the
583 default object is advanced each time an object is retrieved using a Get request. The first three
584 times Locate and Get is executed, the three keys are returned one after the other. When Locate
585 and Get is executed for the fourth time, the first key is again returned. Finally, all keys are
586 destroyed.

587 Note: there is no requirement for a server to implement support for any round-robin based
588 allocation; this test case illustrates a server which supports such a policy.

```
0001 # TIME 0
0002 <RequestMessage>
0003   <RequestHeader>
0004     <ProtocolVersion>
0005       <ProtocolVersionMajor type="Integer" value="1"/>
0006       <ProtocolVersionMinor type="Integer" value="1"/>
0007     </ProtocolVersion>
0008     <BatchCount type="Integer" value="3"/>
0009   </RequestHeader>
0010   <BatchItem>
0011     <Operation type="Enumeration" value="Create"/>
0012     <UniqueBatchItemID type="ByteString" value="75e8bdb337aec40e"/>
0013     <RequestPayload>
0014       <ObjectType type="Enumeration" value="SymmetricKey"/>
0015       <TemplateAttribute>
0016         <Attribute>
0017           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0018           <AttributeValue type="Enumeration" value="AES"/>
0019         </Attribute>
0019       </TemplateAttribute>
0019     </RequestPayload>
0019   </BatchItem>
0019 </BatchMessage>
```

```
0020     <AttributeName type="TextString" value="Cryptographic
Length"/>
0021     <AttributeValue type="Integer" value="256"/>
0022     </Attribute>
0023     <Attribute>
0024     <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0025     <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0026     </Attribute>
0027     <Attribute>
0028     <AttributeName type="TextString" value="Object Group"/>
0029     <AttributeValue type="TextString"
value="RoundRobinTestGroup"/>
0030     </Attribute>
0031     <Attribute>
0032     <AttributeName type="TextString" value="x-ID"/>
0033     <AttributeValue type="TextString" value="TC-153-11-key1"/>
0034     </Attribute>
0035     </TemplateAttribute>
0036     </RequestPayload>
0037     </BatchItem>
0038     <BatchItem>
0039     <Operation type="Enumeration" value="Create"/>
0040     <UniqueBatchItemID type="ByteString" value="ac0e6e56e8d99f66"/>
0041     <RequestPayload>
0042     <ObjectType type="Enumeration" value="SymmetricKey"/>
0043     <TemplateAttribute>
0044     <Attribute>
0045     <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0046     <AttributeValue type="Enumeration" value="AES"/>
0047     </Attribute>
0048     <Attribute>
0049     <AttributeName type="TextString" value="Cryptographic
Length"/>
0050     <AttributeValue type="Integer" value="256"/>
0051     </Attribute>
0052     <Attribute>
0053     <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0054     <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0055     </Attribute>
0056     <Attribute>
0057     <AttributeName type="TextString" value="Object Group"/>
0058     <AttributeValue type="TextString"
value="RoundRobinTestGroup"/>
0059     </Attribute>
0060     <Attribute>
0061     <AttributeName type="TextString" value="x-ID"/>
0062     <AttributeValue type="TextString" value="TC-153-11-key2"/>
0063     </Attribute>
0064     </TemplateAttribute>
0065     </RequestPayload>
0066     </BatchItem>
0067     <BatchItem>
0068     <Operation type="Enumeration" value="Create"/>
0069     <UniqueBatchItemID type="ByteString" value="77e87d356ba09da1"/>
```

0070	<RequestPayload>
0071	<ObjectType type="Enumeration" value="SymmetricKey"/>
0072	<TemplateAttribute>
0073	<Attribute>
0074	<AttributeName type="TextString" value="Cryptographic
0075	Algorithm"/>
0076	<AttributeValue type="Enumeration" value="AES"/>
0077	</Attribute>
0078	<Attribute>
0079	<AttributeName type="TextString" value="Cryptographic
0080	Length"/>
0081	<AttributeValue type="Integer" value="256"/>
0082	</Attribute>
0083	<Attribute>
0084	<AttributeName type="TextString" value="Cryptographic
0085	Usage Mask"/>
0086	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0087	</Attribute>
0088	<Attribute>
0089	<AttributeName type="TextString" value="Object Group"/>
0090	<AttributeValue type="TextString"
0091	value="RoundRobinTestGroup"/>
0092	</Attribute>
0093	</TemplateAttribute>
0094	</RequestPayload>
0095	</BatchItem>
0096	</RequestMessage>
0097	<ResponseMessage>
0098	<ResponseHeader>
0099	<ProtocolVersion>
0100	<ProtocolVersionMajor type="Integer" value="1"/>
0101	<ProtocolVersionMinor type="Integer" value="1"/>
0102	</ProtocolVersion>
0103	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0104	<BatchCount type="Integer" value="3"/>
0105	</ResponseHeader>
0106	<BatchItem>
0107	<Operation type="Enumeration" value="Create"/>
0108	<UniqueBatchItemID type="ByteString" value="75e8bdb337aec40e"/>
0109	<ResultStatus type="Enumeration" value="Success"/>
0110	<ResponsePayload>
0111	<ObjectType type="Enumeration" value="SymmetricKey"/>
0112	<UniqueIdentifier type="TextString"
0113	value="\$UNIQUE_IDENTIFIER_0"/>
0114	</ResponsePayload>
0115	</BatchItem>
0116	<BatchItem>
0117	<Operation type="Enumeration" value="Create"/>
0118	<UniqueBatchItemID type="ByteString" value="ac0e6e56e8d99f66"/>
0119	<ResultStatus type="Enumeration" value="Success"/>
0120	<ResponsePayload>
0121	<ObjectType type="Enumeration" value="SymmetricKey"/>
0122	<UniqueIdentifier type="TextString"

0122	value="\$UNIQUE_IDENTIFIER_1"/>
0123	</ResponsePayload>
0124	</BatchItem>
0125	<BatchItem>
0126	<Operation type="Enumeration" value="Create"/>
0127	<UniqueBatchItemID type="ByteString" value="77e87d356ba09da1"/>
0128	<ResponseStatus type="Enumeration" value="Success"/>
0129	<ResponsePayload>
0130	<ObjectType type="Enumeration" value="SymmetricKey"/>
0131	<UniqueIdentifier type="TextString"
0132	value="\$UNIQUE_IDENTIFIER_2"/>
0133	</ResponsePayload>
0134	</BatchItem>
0135	</ResponseMessage>
0136	# TIME 1
0137	<RequestMessage>
0138	<RequestHeader>
0139	<ProtocolVersion>
0140	<ProtocolVersionMajor type="Integer" value="1"/>
0141	<ProtocolVersionMinor type="Integer" value="1"/>
0142	</ProtocolVersion>
0143	<BatchOrderOption type="Boolean" value="true"/>
0144	<BatchCount type="Integer" value="2"/>
0145	</RequestHeader>
0146	<BatchItem>
0147	<Operation type="Enumeration" value="Locate"/>
0148	<UniqueBatchItemID type="ByteString" value="99e7a6ea0125bb67"/>
0149	<RequestPayload>
0150	<MaximumItems type="Integer" value="1"/>
0151	<ObjectGroupMember type="Enumeration"
0152	value="GroupMemberDefault"/>
0153	<Attribute>
0154	<AttributeName type="TextString" value="Object Group"/>
0155	<AttributeValue type="TextString"
0156	value="RoundRobinTestGroup"/>
0157	</Attribute>
0158	</RequestPayload>
0159	</BatchItem>
0160	<BatchItem>
0161	<Operation type="Enumeration" value="Get"/>
0162	<UniqueBatchItemID type="ByteString" value="0efd9c2e346ee1cb"/>
0163	<RequestPayload>
0164	</RequestPayload>
0165	</BatchItem>
0166	</RequestMessage>
0167	<ResponseMessage>
0168	<ResponseHeader>
0169	<ProtocolVersion>
0170	<ProtocolVersionMajor type="Integer" value="1"/>
0171	<ProtocolVersionMinor type="Integer" value="1"/>
0172	</ProtocolVersion>
0173	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
	<BatchCount type="Integer" value="2"/>
	</ResponseHeader>
	<BatchItem>
	<Operation type="Enumeration" value="Locate"/>
	<UniqueBatchItemID type="ByteString" value="99e7a6ea0125bb67"/>

0174	<ResultStatus type="Enumeration" value="Success"/>
0175	<ResponsePayload>
0176	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0177	</ResponsePayload>
0178	</BatchItem>
0179	<BatchItem>
0180	<Operation type="Enumeration" value="Get"/>
0181	<UniqueBatchItemID type="ByteString" value="0efd9c2e346ee1cb"/>
0182	<ResultStatus type="Enumeration" value="Success"/>
0183	<ResponsePayload>
0184	<ObjectType type="Enumeration" value="SymmetricKey"/>
0185	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0186	<SymmetricKey>
0187	<KeyBlock>
0188	<KeyFormatType type="Enumeration" value="Raw"/>
0189	<KeyValue>
0190	<KeyMaterial type="ByteString"
	value="bd13da8bce07ea6b89c4d110827bf6a8478cf95edca9bbc278ab04f4cbeecff0"/>
0191	</KeyValue>
0192	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0193	<CryptographicLength type="Integer" value="256"/>
0194	</KeyBlock>
0195	</SymmetricKey>
0196	</ResponsePayload>
0197	</BatchItem>
0198	</ResponseMessage>
	# TIME 2
0199	<RequestMessage>
0200	<RequestHeader>
0201	<ProtocolVersion>
0202	<ProtocolVersionMajor type="Integer" value="1"/>
0203	<ProtocolVersionMinor type="Integer" value="1"/>
0204	</ProtocolVersion>
0205	<BatchOrderOption type="Boolean" value="true"/>
0206	<BatchCount type="Integer" value="2"/>
0207	</RequestHeader>
0208	<BatchItem>
0209	<Operation type="Enumeration" value="Locate"/>
0210	<UniqueBatchItemID type="ByteString" value="0303428f37f17b8d"/>
0211	<RequestPayload>
0212	<MaximumItems type="Integer" value="1"/>
0213	<ObjectGroupMember type="Enumeration"
	value="GroupMemberDefault"/>
0214	<Attribute>
0215	<AttributeName type="TextString" value="Object Group"/>
0216	<AttributeValue type="TextString"
	value="RoundRobinTestGroup"/>
0217	</Attribute>
0218	</RequestPayload>
0219	</BatchItem>
0220	<BatchItem>
0221	<Operation type="Enumeration" value="Get"/>
0222	<UniqueBatchItemID type="ByteString" value="dae46b60d9b6459b"/>
0223	<RequestPayload>

0224	</RequestPayload>
0225	</BatchItem>
0226	</RequestMessage>
0227	<ResponseMessage>
0228	<ResponseHeader>
0229	<ProtocolVersion>
0230	<ProtocolVersionMajor type="Integer" value="1"/>
0231	<ProtocolVersionMinor type="Integer" value="1"/>
0232	</ProtocolVersion>
0233	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0234	<BatchCount type="Integer" value="2"/>
0235	</ResponseHeader>
0236	<BatchItem>
0237	<Operation type="Enumeration" value="Locate"/>
0238	<UniqueBatchItemID type="ByteString" value="0303428f37f17b8d"/>
0239	<ResultStatus type="Enumeration" value="Success"/>
0240	<ResponsePayload>
0241	<UniqueIdentifier type="TextString"
0242	value="\$UNIQUE_IDENTIFIER_1"/>
0243	</ResponsePayload>
0244	</BatchItem>
0245	<BatchItem>
0246	<Operation type="Enumeration" value="Get"/>
0247	<UniqueBatchItemID type="ByteString" value="dae46b60d9b6459b"/>
0248	<ResultStatus type="Enumeration" value="Success"/>
0249	<ResponsePayload>
0250	<ObjectType type="Enumeration" value="SymmetricKey"/>
0251	<UniqueIdentifier type="TextString"
0252	value="\$UNIQUE_IDENTIFIER_1"/>
0253	<SymmetricKey>
0254	<KeyBlock>
0255	<KeyFormatType type="Enumeration" value="Raw"/>
0256	<KeyValue>
0257	<KeyMaterial type="ByteString"
0258	value="430bfb0cbc273e15326e3a23965f7704a13af37a642c37026c9a59694c83b7a3"/>
0259	</KeyValue>
0260	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0261	<CryptographicLength type="Integer" value="256"/>
0262	</KeyBlock>
0263	</SymmetricKey>
0264	</ResponsePayload>
0265	</BatchItem>
0266	</ResponseMessage>
0267	# TIME 3
0268	<RequestMessage>
0269	<RequestHeader>
0270	<ProtocolVersion>
0271	<ProtocolVersionMajor type="Integer" value="1"/>
0272	<ProtocolVersionMinor type="Integer" value="1"/>
0273	</ProtocolVersion>
0274	<BatchOrderOption type="Boolean" value="true"/>
0275	<BatchCount type="Integer" value="2"/>
0276	</RequestHeader>
0277	<BatchItem>
0278	<Operation type="Enumeration" value="Locate"/>
0279	<UniqueBatchItemID type="ByteString" value="863c27d7a0d3da5e"/>

0276	<RequestPayload>
0277	<MaximumItems type="Integer" value="1"/>
0278	<ObjectGroupMember type="Enumeration"
	value="GroupMemberDefault"/>
0279	<Attribute>
0280	<AttributeName type="TextString" value="Object Group"/>
0281	<AttributeValue type="TextString"
	value="RoundRobinTestGroup"/>
0282	</Attribute>
0283	</RequestPayload>
0284	</BatchItem>
0285	<BatchItem>
0286	<Operation type="Enumeration" value="Get"/>
0287	<UniqueBatchItemID type="ByteString" value="c4617b3205e96fb2"/>
0288	<RequestPayload>
0289	</RequestPayload>
0290	</BatchItem>
0291	</RequestMessage>
0292	<ResponseMessage>
0293	<ResponseHeader>
0294	<ProtocolVersion>
0295	<ProtocolVersionMajor type="Integer" value="1"/>
0296	<ProtocolVersionMinor type="Integer" value="1"/>
0297	</ProtocolVersion>
0298	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0299	<BatchCount type="Integer" value="2"/>
0300	</ResponseHeader>
0301	<BatchItem>
0302	<Operation type="Enumeration" value="Locate"/>
0303	<UniqueBatchItemID type="ByteString" value="863c27d7a0d3da5e"/>
0304	<ResultStatus type="Enumeration" value="Success"/>
0305	<ResponsePayload>
0306	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0307	</ResponsePayload>
0308	</BatchItem>
0309	<BatchItem>
0310	<Operation type="Enumeration" value="Get"/>
0311	<UniqueBatchItemID type="ByteString" value="c4617b3205e96fb2"/>
0312	<ResultStatus type="Enumeration" value="Success"/>
0313	<ResponsePayload>
0314	<ObjectType type="Enumeration" value="SymmetricKey"/>
0315	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0316	<SymmetricKey>
0317	<KeyBlock>
0318	<KeyFormatType type="Enumeration" value="Raw"/>
0319	<KeyValue>
0320	<KeyMaterial type="ByteString"
	value="a51b38e400168a25f2f122d7b8543a00daf022e61677a08a33a834f5f52c3097"/>
0321	</KeyValue>
0322	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0323	<CryptographicLength type="Integer" value="256"/>
0324	</KeyBlock>
0325	</SymmetricKey>
0326	</ResponsePayload>

0327	</BatchItem>
0328	</ResponseMessage>
# TIME 4	
0329	<RequestMessage>
0330	<RequestHeader>
0331	<ProtocolVersion>
0332	<ProtocolVersionMajor type="Integer" value="1"/>
0333	<ProtocolVersionMinor type="Integer" value="1"/>
0334	</ProtocolVersion>
0335	<BatchOrderOption type="Boolean" value="true"/>
0336	<BatchCount type="Integer" value="2"/>
0337	</RequestHeader>
0338	<BatchItem>
0339	<Operation type="Enumeration" value="Locate"/>
0340	<UniqueBatchItemID type="ByteString" value="f1ce9893ee5bde19"/>
0341	<RequestPayload>
0342	<MaximumItems type="Integer" value="1"/>
0343	<ObjectGroupMember type="Enumeration"
	value="GroupMemberDefault"/>
0344	<Attribute>
0345	<AttributeName type="TextString" value="Object Group"/>
0346	<AttributeValue type="TextString"
	value="RoundRobinTestGroup"/>
0347	</Attribute>
0348	</RequestPayload>
0349	</BatchItem>
0350	<BatchItem>
0351	<Operation type="Enumeration" value="Get"/>
0352	<UniqueBatchItemID type="ByteString" value="9a18dd11cc6ce394"/>
0353	<RequestPayload>
0354	</RequestPayload>
0355	</BatchItem>
0356	</RequestMessage>
0357	<ResponseMessage>
0358	<ResponseHeader>
0359	<ProtocolVersion>
0360	<ProtocolVersionMajor type="Integer" value="1"/>
0361	<ProtocolVersionMinor type="Integer" value="1"/>
0362	</ProtocolVersion>
0363	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0364	<BatchCount type="Integer" value="2"/>
0365	</ResponseHeader>
0366	<BatchItem>
0367	<Operation type="Enumeration" value="Locate"/>
0368	<UniqueBatchItemID type="ByteString" value="f1ce9893ee5bde19"/>
0369	<ResultStatus type="Enumeration" value="Success"/>
0370	<ResponsePayload>
0371	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0372	</ResponsePayload>
0373	</BatchItem>
0374	<BatchItem>
0375	<Operation type="Enumeration" value="Get"/>
0376	<UniqueBatchItemID type="ByteString" value="9a18dd11cc6ce394"/>
0377	<ResultStatus type="Enumeration" value="Success"/>
0378	<ResponsePayload>
0379	<ObjectType type="Enumeration" value="SymmetricKey"/>

0380	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0381	<SymmetricKey>
0382	<KeyBlock>
0383	<KeyFormatType type="Enumeration" value="Raw"/>
0384	<KeyValue>
0385	<KeyMaterial type="ByteString"
	value="bd13da8bce07ea6b89c4d110827bf6a8478cf95edca9bbc278ab04f4cbeecff0"/>
0386	</KeyValue>
0387	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0388	<CryptographicLength type="Integer" value="256"/>
0389	</KeyBlock>
0390	</SymmetricKey>
0391	</ResponsePayload>
0392	</BatchItem>
0393	</ResponseMessage>
	# TIME 5
0394	<RequestMessage>
0395	<RequestHeader>
0396	<ProtocolVersion>
0397	<ProtocolVersionMajor type="Integer" value="1"/>
0398	<ProtocolVersionMinor type="Integer" value="1"/>
0399	</ProtocolVersion>
0400	<BatchErrorContinuationOption type="Enumeration"
	value="Continue"/>
0401	<BatchOrderOption type="Boolean" value="true"/>
0402	<BatchCount type="Integer" value="3"/>
0403	</RequestHeader>
0404	<BatchItem>
0405	<Operation type="Enumeration" value="Destroy"/>
0406	<UniqueBatchItemID type="ByteString" value="f4cf0a5614786eb7"/>
0407	<RequestPayload>
0408	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0409	</RequestPayload>
0410	</BatchItem>
0411	<BatchItem>
0412	<Operation type="Enumeration" value="Destroy"/>
0413	<UniqueBatchItemID type="ByteString" value="dd55da10ebe91928"/>
0414	<RequestPayload>
0415	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0416	</RequestPayload>
0417	</BatchItem>
0418	<BatchItem>
0419	<Operation type="Enumeration" value="Destroy"/>
0420	<UniqueBatchItemID type="ByteString" value="18334af52fee87fa"/>
0421	<RequestPayload>
0422	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0423	</RequestPayload>
0424	</BatchItem>
0425	</RequestMessage>
0426	<ResponseMessage>
0427	<ResponseHeader>
0428	<ProtocolVersion>

0429	<ProtocolVersionMajor type="Integer" value="1"/>
0430	<ProtocolVersionMinor type="Integer" value="1"/>
0431	</ProtocolVersion>
0432	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0433	<BatchCount type="Integer" value="3"/>
0434	</ResponseHeader>
0435	<BatchItem>
0436	<Operation type="Enumeration" value="Destroy"/>
0437	<UniqueBatchItemID type="ByteString" value="f4cf0a5614786eb7"/>
0438	<ResultStatus type="Enumeration" value="Success"/>
0439	<ResponsePayload>
0440	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0441	</ResponsePayload>
0442	</BatchItem>
0443	<BatchItem>
0444	<Operation type="Enumeration" value="Destroy"/>
0445	<UniqueBatchItemID type="ByteString" value="dd55da10ebe91928"/>
0446	<ResultStatus type="Enumeration" value="Success"/>
0447	<ResponsePayload>
0448	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0449	</ResponsePayload>
0450	</BatchItem>
0451	<BatchItem>
0452	<Operation type="Enumeration" value="Destroy"/>
0453	<UniqueBatchItemID type="ByteString" value="18334af52fee87fa"/>
0454	<ResultStatus type="Enumeration" value="Success"/>
0455	<ResponsePayload>
0456	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0457	</ResponsePayload>
0458	</BatchItem>
0459	</ResponseMessage>

589

590 2.2.33 TC-161-11 - Discover Versions

591 Exercise the Discover Versions operation in different ways in order to find out which versions a
592 server supports, as well as to get a list of versions supported by both client and server.

593 This test case shows the expected responses from a KMIP 1.2 server that supports versions 1.1
594 and 1.0, with 1.1 being the preferred version.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="DiscoverVersions"/>
0011	<RequestPayload>

0012	</RequestPayload>
0013	</BatchItem>
0014	</RequestMessage>
0015	<ResponseMessage>
0016	<ResponseHeader>
0017	<ProtocolVersion>
0018	<ProtocolVersionMajor type="Integer" value="1"/>
0019	<ProtocolVersionMinor type="Integer" value="1"/>
0020	</ProtocolVersion>
0021	<TimeStamp type="DateTime" value="2011-12-01T08:46:15+00:00"/>
0022	<BatchCount type="Integer" value="1"/>
0023	</ResponseHeader>
0024	<BatchItem>
0025	<Operation type="Enumeration" value="DiscoverVersions"/>
0026	<ResultStatus type="Enumeration" value="Success"/>
0027	<ResponsePayload>
0028	<ProtocolVersion>
0029	<ProtocolVersionMajor type="Integer" value="1"/>
0030	<ProtocolVersionMinor type="Integer" value="1"/>
0031	</ProtocolVersion>
0032	<ProtocolVersion>
0033	<ProtocolVersionMajor type="Integer" value="1"/>
0034	<ProtocolVersionMinor type="Integer" value="0"/>
0035	</ProtocolVersion>
0036	</ResponsePayload>
0037	</BatchItem>
0038	</ResponseMessage>
# TIME 1	
0039	<RequestMessage>
0040	<RequestHeader>
0041	<ProtocolVersion>
0042	<ProtocolVersionMajor type="Integer" value="1"/>
0043	<ProtocolVersionMinor type="Integer" value="1"/>
0044	</ProtocolVersion>
0045	<BatchCount type="Integer" value="1"/>
0046	</RequestHeader>
0047	<BatchItem>
0048	<Operation type="Enumeration" value="DiscoverVersions"/>
0049	<RequestPayload>
0050	<ProtocolVersion>
0051	<ProtocolVersionMajor type="Integer" value="1"/>
0052	<ProtocolVersionMinor type="Integer" value="0"/>
0053	</ProtocolVersion>
0054	</RequestPayload>
0055	</BatchItem>
0056	</RequestMessage>
0057	<ResponseMessage>
0058	<ResponseHeader>
0059	<ProtocolVersion>
0060	<ProtocolVersionMajor type="Integer" value="1"/>
0061	<ProtocolVersionMinor type="Integer" value="1"/>
0062	</ProtocolVersion>
0063	<TimeStamp type="DateTime" value="2011-06-24T12:52:18+00:00"/>
0064	<BatchCount type="Integer" value="1"/>
0065	</ResponseHeader>
0066	<BatchItem>

0067	<Operation type="Enumeration" value="DiscoverVersions"/>
0068	<ResultStatus type="Enumeration" value="Success"/>
0069	<ResponsePayload>
0070	<ProtocolVersion>
0071	<ProtocolVersionMajor type="Integer" value="1"/>
0072	<ProtocolVersionMinor type="Integer" value="0"/>
0073	</ProtocolVersion>
0074	</ResponsePayload>
0075	</BatchItem>
0076	</ResponseMessage>
# TIME 2	
0077	<RequestMessage>
0078	<RequestHeader>
0079	<ProtocolVersion>
0080	<ProtocolVersionMajor type="Integer" value="1"/>
0081	<ProtocolVersionMinor type="Integer" value="1"/>
0082	</ProtocolVersion>
0083	<BatchCount type="Integer" value="1"/>
0084	</RequestHeader>
0085	<BatchItem>
0086	<Operation type="Enumeration" value="DiscoverVersions"/>
0087	<RequestPayload>
0088	<ProtocolVersion>
0089	<ProtocolVersionMajor type="Integer" value="1"/>
0090	<ProtocolVersionMinor type="Integer" value="1"/>
0091	</ProtocolVersion>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="1"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2011-12-01T08:46:15+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="DiscoverVersions"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<ProtocolVersion>
0109	<ProtocolVersionMajor type="Integer" value="1"/>
0110	<ProtocolVersionMinor type="Integer" value="1"/>
0111	</ProtocolVersion>
0112	</ResponsePayload>
0113	</BatchItem>
0114	</ResponseMessage>
# TIME 3	
0115	<RequestMessage>
0116	<RequestHeader>
0117	<ProtocolVersion>
0118	<ProtocolVersionMajor type="Integer" value="1"/>
0119	<ProtocolVersionMinor type="Integer" value="1"/>
0120	</ProtocolVersion>

0121	<BatchCount type="Integer" value="1"/>
0122	</RequestHeader>
0123	<BatchItem>
0124	<Operation type="Enumeration" value="DiscoverVersions"/>
0125	<RequestPayload>
0126	<ProtocolVersion>
0127	<ProtocolVersionMajor type="Integer" value="9"/>
0128	<ProtocolVersionMinor type="Integer" value="31"/>
0129	</ProtocolVersion>
0130	</RequestPayload>
0131	</BatchItem>
0132	</RequestMessage>
0133	<ResponseMessage>
0134	<ResponseHeader>
0135	<ProtocolVersion>
0136	<ProtocolVersionMajor type="Integer" value="1"/>
0137	<ProtocolVersionMinor type="Integer" value="1"/>
0138	</ProtocolVersion>
0139	<TimeStamp type="DateTime" value="2011-12-01T08:46:15+00:00"/>
0140	<BatchCount type="Integer" value="1"/>
0141	</ResponseHeader>
0142	<BatchItem>
0143	<Operation type="Enumeration" value="DiscoverVersions"/>
0144	<ResultStatus type="Enumeration" value="Success"/>
0145	<ResponsePayload>
0146	</ResponsePayload>
0147	</BatchItem>
0148	</ResponseMessage>

595

596 2.2.34 TC-171-11 - Handling of Attributes and Attribute Index Values

597 This test case illustrates the changes in Attribute and Attribute Index handling introduced in
598 KMIP-1.1. A symmetric key is created on the server, and two Name attributes and the Contact
599 Information attribute is specified for the key. A Get Attributes request containing the Object
600 Type attribute name twice is sent, but this operation fails since a single Attribute Name cannot
601 be specified more than once in a Get Attributes request. The Object Type Attribute is then
602 requested once, and this request succeeds. Thereafter, the Contact Information Attribute is
603 modified, with the Attribute Index value of 0 specified. The Name attribute is deleted without
604 specifying the Attribute Index which succeeds (which would have failed under KMIP-1.0). Finally,
605 the created key is destroyed.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>

0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic Length"/>
0020	<AttributeValue type="Integer" value="256"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="TC-171-11-name1"/>
0030	<NameType type="Enumeration" value="UninterpretedTextString"/>
0031	</AttributeValue>
0032	</Attribute>
0033	<Attribute>
0034	<AttributeName type="TextString" value="Name"/>
0035	<AttributeValue>
0036	<NameValue type="TextString" value="TC-171-11-name2"/>
0037	<NameType type="Enumeration" value="UninterpretedTextString"/>
0038	</AttributeValue>
0039	</Attribute>
0040	<Attribute>
0041	<AttributeName type="TextString" value="Contact Information"/>
0042	<AttributeValue type="TextString" value="admin@localhost"/>
0043	</Attribute>
0044	</TemplateAttribute>
0045	</RequestPayload>
0046	</BatchItem>
0047	</RequestMessage>
0048	<ResponseMessage>
0049	<ResponseHeader>
0050	<ProtocolVersion>
0051	<ProtocolVersionMajor type="Integer" value="1"/>
0052	<ProtocolVersionMinor type="Integer" value="1"/>
0053	</ProtocolVersion>
0054	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0055	<BatchCount type="Integer" value="1"/>
0056	</ResponseHeader>
0057	<BatchItem>
0058	<Operation type="Enumeration" value="Create"/>
0059	<ResultStatus type="Enumeration" value="Success"/>
0060	<ResponsePayload>
0061	<ObjectType type="Enumeration" value="SymmetricKey"/>

0062	<UniqueIdentifier type="TextString"
0063	value="\$UNIQUE_IDENTIFIER_0"/>
0064	</ResponsePayload>
0065	</BatchItem>
	</ResponseMessage>
	# TIME 1
0066	<RequestMessage>
0067	<RequestHeader>
0068	<ProtocolVersion>
0069	<ProtocolVersionMajor type="Integer" value="1"/>
0070	<ProtocolVersionMinor type="Integer" value="1"/>
0071	</ProtocolVersion>
0072	<BatchCount type="Integer" value="1"/>
0073	</RequestHeader>
0074	<BatchItem>
0075	<Operation type="Enumeration" value="GetAttributes"/>
0076	<RequestPayload>
0077	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0078	<AttributeName type="TextString" value="Object Type"/>
0079	<AttributeName type="TextString" value="Object Type"/>
0080	</RequestPayload>
0081	</BatchItem>
0082	</RequestMessage>
0083	<ResponseMessage>
0084	<ResponseHeader>
0085	<ProtocolVersion>
0086	<ProtocolVersionMajor type="Integer" value="1"/>
0087	<ProtocolVersionMinor type="Integer" value="1"/>
0088	</ProtocolVersion>
0089	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0090	<BatchCount type="Integer" value="1"/>
0091	</ResponseHeader>
0092	<BatchItem>
0093	<Operation type="Enumeration" value="GetAttributes"/>
0094	<ResultStatus type="Enumeration" value="OperationFailed"/>
0095	<ResultReason type="Enumeration" value="InvalidMessage"/>
0096	<ResultMessage type="TextString" value="Attribute Name specified
	more than once: Object Type"/>
0097	</BatchItem>
0098	</ResponseMessage>
	# TIME 2
0099	<RequestMessage>
0100	<RequestHeader>
0101	<ProtocolVersion>
0102	<ProtocolVersionMajor type="Integer" value="1"/>
0103	<ProtocolVersionMinor type="Integer" value="1"/>
0104	</ProtocolVersion>
0105	<BatchCount type="Integer" value="1"/>
0106	</RequestHeader>
0107	<BatchItem>
0108	<Operation type="Enumeration" value="GetAttributes"/>
0109	<RequestPayload>
0110	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0111	<AttributeName type="TextString" value="Object Type"/>

0112	</RequestPayload>
0113	</BatchItem>
0114	</RequestMessage>
0115	<ResponseMessage>
0116	<ResponseHeader>
0117	<ProtocolVersion>
0118	<ProtocolVersionMajor type="Integer" value="1"/>
0119	<ProtocolVersionMinor type="Integer" value="1"/>
0120	</ProtocolVersion>
0121	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0122	<BatchCount type="Integer" value="1"/>
0123	</ResponseHeader>
0124	<BatchItem>
0125	<Operation type="Enumeration" value="GetAttributes"/>
0126	<ResultStatus type="Enumeration" value="Success"/>
0127	<ResponsePayload>
0128	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0129	<Attribute>
0130	<AttributeName type="TextString" value="Object Type"/>
0131	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0132	</Attribute>
0133	</ResponsePayload>
0134	</BatchItem>
0135	</ResponseMessage>
# TIME 3	
0136	<RequestMessage>
0137	<RequestHeader>
0138	<ProtocolVersion>
0139	<ProtocolVersionMajor type="Integer" value="1"/>
0140	<ProtocolVersionMinor type="Integer" value="1"/>
0141	</ProtocolVersion>
0142	<BatchCount type="Integer" value="1"/>
0143	</RequestHeader>
0144	<BatchItem>
0145	<Operation type="Enumeration" value="ModifyAttribute"/>
0146	<RequestPayload>
0147	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0148	<Attribute>
0149	<AttributeName type="TextString" value="Contact Information"/>
0150	<AttributeIndex type="Integer" value="0"/>
0151	<AttributeValue type="TextString" value="donald@localhost"/>
0152	</Attribute>
0153	</RequestPayload>
0154	</BatchItem>
0155	</RequestMessage>
0156	<ResponseMessage>
0157	<ResponseHeader>
0158	<ProtocolVersion>
0159	<ProtocolVersionMajor type="Integer" value="1"/>
0160	<ProtocolVersionMinor type="Integer" value="1"/>
0161	</ProtocolVersion>
0162	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0163	<BatchCount type="Integer" value="1"/>

0164	</ResponseHeader>
0165	<BatchItem>
0166	<Operation type="Enumeration" value="ModifyAttribute"/>
0167	<ResultStatus type="Enumeration" value="Success"/>
0168	<ResponsePayload>
0169	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0170	<Attribute>
0171	<AttributeName type="TextString" value="Contact
	Information"/>
0172	<AttributeValue type="TextString" value="donald@localhost"/>
0173	</Attribute>
0174	</ResponsePayload>
0175	</BatchItem>
0176	</ResponseMessage>
# TIME 4	
0177	<RequestMessage>
0178	<RequestHeader>
0179	<ProtocolVersion>
0180	<ProtocolVersionMajor type="Integer" value="1"/>
0181	<ProtocolVersionMinor type="Integer" value="1"/>
0182	</ProtocolVersion>
0183	<BatchCount type="Integer" value="1"/>
0184	</RequestHeader>
0185	<BatchItem>
0186	<Operation type="Enumeration" value="DeleteAttribute"/>
0187	<RequestPayload>
0188	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0189	<AttributeName type="TextString" value="Name"/>
0190	</RequestPayload>
0191	</BatchItem>
0192	</RequestMessage>
0193	<ResponseMessage>
0194	<ResponseHeader>
0195	<ProtocolVersion>
0196	<ProtocolVersionMajor type="Integer" value="1"/>
0197	<ProtocolVersionMinor type="Integer" value="1"/>
0198	</ProtocolVersion>
0199	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0200	<BatchCount type="Integer" value="1"/>
0201	</ResponseHeader>
0202	<BatchItem>
0203	<Operation type="Enumeration" value="DeleteAttribute"/>
0204	<ResultStatus type="Enumeration" value="Success"/>
0205	<ResponsePayload>
0206	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0207	<Attribute>
0208	<AttributeName type="TextString" value="Name"/>
0209	<AttributeValue>
0210	<NameValue type="TextString" value="TC-171-11-name1"/>
0211	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0212	</AttributeValue>
0213	</Attribute>
0214	</ResponsePayload>

0215	</BatchItem>
0216	</ResponseMessage>
# TIME 5	
0217	<RequestMessage>
0218	<RequestHeader>
0219	<ProtocolVersion>
0220	<ProtocolVersionMajor type="Integer" value="1"/>
0221	<ProtocolVersionMinor type="Integer" value="1"/>
0222	</ProtocolVersion>
0223	<BatchCount type="Integer" value="1"/>
0224	</RequestHeader>
0225	<BatchItem>
0226	<Operation type="Enumeration" value="Destroy"/>
0227	<RequestPayload>
0228	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0229	</RequestPayload>
0230	</BatchItem>
0231	</RequestMessage>
0232	<ResponseMessage>
0233	<ResponseHeader>
0234	<ProtocolVersion>
0235	<ProtocolVersionMajor type="Integer" value="1"/>
0236	<ProtocolVersionMinor type="Integer" value="1"/>
0237	</ProtocolVersion>
0238	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0239	<BatchCount type="Integer" value="1"/>
0240	</ResponseHeader>
0241	<BatchItem>
0242	<Operation type="Enumeration" value="Destroy"/>
0243	<ResultStatus type="Enumeration" value="Success"/>
0244	<ResponsePayload>
0245	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0246	</ResponsePayload>
0247	</BatchItem>
0248	</ResponseMessage>

606

607 2.2.35 TC-181-11 - Digests of Symmetric Keys

608 Exercise the Digest attribute by registering two symmetric keys with the same key material but
609 using different Key Format Type. The Digest Value for the key with the Key Format Type set to
610 Transparent Symmetric Key is calculated on the TTLV-encoded Key Material structure, whereas
611 the Digest Value for the key registered in the Raw Key Format Type is calculated on the raw Key
612 Material Byte String. The server calculates the value of the mandatory Digest attribute instance
613 using the Key Format Type used by the client when registering the keys. Thereafter, the client
614 asks the server to create a symmetric key using the Create operation. In this situation, it is up to
615 the server to choose what Key Format Type of the created key it uses to calculate the Digest
616 Value.

617 Note: This test case assumes a server that does not compute any additional Digest attributes
618 using another Hashing Algorithm and/or Key Format Type. A server is permitted to provide
619 multiple Digest attributes.

620

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Length"/>
0022	<AttributeValue type="Integer" value="256"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Cryptographic
0026	Usage Mask"/>
0027	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="x-ID"/>
0031	<AttributeValue type="TextString" value="TC-181-11-key1"/>
0032	</Attribute>
0033	</TemplateAttribute>
0034	<SymmetricKey>
0035	<KeyBlock>
0036	<KeyFormatType type="Enumeration" value="Raw"/>
0037	<KeyValue>
0038	<KeyMaterial type="ByteString"
0039	value="0000111122223333444455556666777788889999aaaabbbbccccdddeeeef
0040	fff"/>
0041	</KeyValue>
0042	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0043	<CryptographicLength type="Integer" value="256"/>
0044	</KeyBlock>
	</SymmetricKey>
	</RequestPayload>
	</BatchItem>
	</RequestMessage>
0044	<ResponseMessage>

0045	<ResponseHeader>
0046	<ProtocolVersion>
0047	<ProtocolVersionMajor type="Integer" value="1"/>
0048	<ProtocolVersionMinor type="Integer" value="1"/>
0049	</ProtocolVersion>
0050	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0051	<BatchCount type="Integer" value="1"/>
0052	</ResponseHeader>
0053	<BatchItem>
0054	<Operation type="Enumeration" value="Register"/>
0055	<ResultStatus type="Enumeration" value="Success"/>
0056	<ResponsePayload>
0057	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0058	</ResponsePayload>
0059	</BatchItem>
0060	</ResponseMessage>
	# TIME 1
0061	<RequestMessage>
0062	<RequestHeader>
0063	<ProtocolVersion>
0064	<ProtocolVersionMajor type="Integer" value="1"/>
0065	<ProtocolVersionMinor type="Integer" value="1"/>
0066	</ProtocolVersion>
0067	<BatchCount type="Integer" value="1"/>
0068	</RequestHeader>
0069	<BatchItem>
0070	<Operation type="Enumeration" value="GetAttributes"/>
0071	<RequestPayload>
0072	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0073	<AttributeName type="TextString" value="Digest"/>
0074	</RequestPayload>
0075	</BatchItem>
0076	</RequestMessage>
0077	<ResponseMessage>
0078	<ResponseHeader>
0079	<ProtocolVersion>
0080	<ProtocolVersionMajor type="Integer" value="1"/>
0081	<ProtocolVersionMinor type="Integer" value="1"/>
0082	</ProtocolVersion>
0083	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0084	<BatchCount type="Integer" value="1"/>
0085	</ResponseHeader>
0086	<BatchItem>
0087	<Operation type="Enumeration" value="GetAttributes"/>
0088	<ResultStatus type="Enumeration" value="Success"/>
0089	<ResponsePayload>
0090	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0091	<Attribute>
0092	<AttributeName type="TextString" value="Digest"/>
0093	<AttributeValue>
0094	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0095	<DigestValue type="ByteString"
	value="6c064fe051add1ledc07727b594eb48711df843e08445bba2cd786bc16bc58e8"/>

0096	<KeyFormatType type="Enumeration" value="Raw"/>
0097	</AttributeValue>
0098	</Attribute>
0099	</ResponsePayload>
0100	</BatchItem>
0101	</ResponseMessage>
# TIME 2	
0102	<RequestMessage>
0103	<RequestHeader>
0104	<ProtocolVersion>
0105	<ProtocolVersionMajor type="Integer" value="1"/>
0106	<ProtocolVersionMinor type="Integer" value="1"/>
0107	</ProtocolVersion>
0108	<BatchCount type="Integer" value="1"/>
0109	</RequestHeader>
0110	<BatchItem>
0111	<Operation type="Enumeration" value="Register"/>
0112	<RequestPayload>
0113	<ObjectType type="Enumeration" value="SymmetricKey"/>
0114	<TemplateAttribute>
0115	<Attribute>
0116	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0117	<AttributeValue type="Enumeration" value="AES"/>
0118	</Attribute>
0119	<Attribute>
0120	<AttributeName type="TextString" value="Cryptographic Length"/>
0121	<AttributeValue type="Integer" value="256"/>
0122	</Attribute>
0123	<Attribute>
0124	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0125	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0126	</Attribute>
0127	<Attribute>
0128	<AttributeName type="TextString" value="x-ID"/>
0129	<AttributeValue type="TextString" value="TC-181-11-key2"/>
0130	</Attribute>
0131	</TemplateAttribute>
0132	<SymmetricKey>
0133	<KeyBlock>
0134	<KeyFormatType type="Enumeration" value="TransparentSymmetricKey"/>
0135	<KeyValue>
0136	<KeyMaterial>
0137	<Key type="ByteString" value="0000111122223333444455556666777788889999aaaabbbbccccdddeeeef fff"/>
0138	</KeyMaterial>
0139	</KeyValue>
0140	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0141	<CryptographicLength type="Integer" value="256"/>
0142	</KeyBlock>
0143	</SymmetricKey>
0144	</RequestPayload>
0145	</BatchItem>

0146	</RequestMessage>
0147	<ResponseMessage>
0148	<ResponseHeader>
0149	<ProtocolVersion>
0150	<ProtocolVersionMajor type="Integer" value="1"/>
0151	<ProtocolVersionMinor type="Integer" value="1"/>
0152	</ProtocolVersion>
0153	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0154	<BatchCount type="Integer" value="1"/>
0155	</ResponseHeader>
0156	<BatchItem>
0157	<Operation type="Enumeration" value="Register"/>
0158	<ResultStatus type="Enumeration" value="Success"/>
0159	<ResponsePayload>
0160	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0161	</ResponsePayload>
0162	</BatchItem>
0163	</ResponseMessage>
# TIME 3	
0164	<RequestMessage>
0165	<RequestHeader>
0166	<ProtocolVersion>
0167	<ProtocolVersionMajor type="Integer" value="1"/>
0168	<ProtocolVersionMinor type="Integer" value="1"/>
0169	</ProtocolVersion>
0170	<BatchCount type="Integer" value="1"/>
0171	</RequestHeader>
0172	<BatchItem>
0173	<Operation type="Enumeration" value="GetAttributes"/>
0174	<RequestPayload>
0175	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0176	<AttributeName type="TextString" value="Digest"/>
0177	</RequestPayload>
0178	</BatchItem>
0179	</RequestMessage>
0180	<ResponseMessage>
0181	<ResponseHeader>
0182	<ProtocolVersion>
0183	<ProtocolVersionMajor type="Integer" value="1"/>
0184	<ProtocolVersionMinor type="Integer" value="1"/>
0185	</ProtocolVersion>
0186	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0187	<BatchCount type="Integer" value="1"/>
0188	</ResponseHeader>
0189	<BatchItem>
0190	<Operation type="Enumeration" value="GetAttributes"/>
0191	<ResultStatus type="Enumeration" value="Success"/>
0192	<ResponsePayload>
0193	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0194	<Attribute>
0195	<AttributeName type="TextString" value="Digest"/>
0196	<AttributeValue>
0197	<HashingAlgorithm type="Enumeration" value="SHA_256"/>

0198	<code><DigestValue type="ByteString"</code>
	<code>value="499ce96ff6f5e19fe9fe7a2fe4c3e92b88db0001a4e8df28d9966856b6c4b</code>
	<code>87c"/></code>
0199	<code><KeyFormatType type="Enumeration"</code>
	<code>value="TransparentSymmetricKey"/></code>
0200	<code></AttributeValue></code>
0201	<code></Attribute></code>
0202	<code></ResponsePayload></code>
0203	<code></BatchItem></code>
0204	<code></ResponseMessage></code>
# TIME 4	
0205	<code><RequestMessage></code>
0206	<code><RequestHeader></code>
0207	<code><ProtocolVersion></code>
0208	<code><ProtocolVersionMajor type="Integer" value="1"/></code>
0209	<code><ProtocolVersionMinor type="Integer" value="1"/></code>
0210	<code></ProtocolVersion></code>
0211	<code><BatchCount type="Integer" value="1"/></code>
0212	<code></RequestHeader></code>
0213	<code><BatchItem></code>
0214	<code><Operation type="Enumeration" value="Create"/></code>
0215	<code><RequestPayload></code>
0216	<code><ObjectType type="Enumeration" value="SymmetricKey"/></code>
0217	<code><TemplateAttribute></code>
0218	<code><Attribute></code>
0219	<code><AttributeName type="TextString" value="Cryptographic</code>
	<code>Algorithm"/></code>
0220	<code><AttributeValue type="Enumeration" value="AES"/></code>
0221	<code></Attribute></code>
0222	<code><Attribute></code>
0223	<code><AttributeName type="TextString" value="Cryptographic</code>
	<code>Length"/></code>
0224	<code><AttributeValue type="Integer" value="256"/></code>
0225	<code></Attribute></code>
0226	<code><Attribute></code>
0227	<code><AttributeName type="TextString" value="Cryptographic</code>
	<code>Usage Mask"/></code>
0228	<code><AttributeValue type="Integer" value="Decrypt Encrypt"/></code>
0229	<code></Attribute></code>
0230	<code><Attribute></code>
0231	<code><AttributeName type="TextString" value="x-ID"/></code>
0232	<code><AttributeValue type="TextString" value="TC-181-11-key3"/></code>
0233	<code></Attribute></code>
0234	<code></TemplateAttribute></code>
0235	<code></RequestPayload></code>
0236	<code></BatchItem></code>
0237	<code></RequestMessage></code>
0238	<code><ResponseMessage></code>
0239	<code><ResponseHeader></code>
0240	<code><ProtocolVersion></code>
0241	<code><ProtocolVersionMajor type="Integer" value="1"/></code>
0242	<code><ProtocolVersionMinor type="Integer" value="1"/></code>
0243	<code></ProtocolVersion></code>
0244	<code><TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/></code>
0245	<code><BatchCount type="Integer" value="1"/></code>
0246	<code></ResponseHeader></code>
0247	<code><BatchItem></code>

0248	<Operation type="Enumeration" value="Create"/>
0249	<ResultStatus type="Enumeration" value="Success"/>
0250	<ResponsePayload>
0251	<ObjectType type="Enumeration" value="SymmetricKey"/>
0252	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0253	</ResponsePayload>
0254	</BatchItem>
0255	</ResponseMessage>
	# TIME 5
0256	<RequestMessage>
0257	<RequestHeader>
0258	<ProtocolVersion>
0259	<ProtocolVersionMajor type="Integer" value="1"/>
0260	<ProtocolVersionMinor type="Integer" value="1"/>
0261	</ProtocolVersion>
0262	<BatchCount type="Integer" value="1"/>
0263	</RequestHeader>
0264	<BatchItem>
0265	<Operation type="Enumeration" value="GetAttributes"/>
0266	<RequestPayload>
0267	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0268	<AttributeName type="TextString" value="Digest"/>
0269	</RequestPayload>
0270	</BatchItem>
0271	</RequestMessage>
0272	<ResponseMessage>
0273	<ResponseHeader>
0274	<ProtocolVersion>
0275	<ProtocolVersionMajor type="Integer" value="1"/>
0276	<ProtocolVersionMinor type="Integer" value="1"/>
0277	</ProtocolVersion>
0278	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0279	<BatchCount type="Integer" value="1"/>
0280	</ResponseHeader>
0281	<BatchItem>
0282	<Operation type="Enumeration" value="GetAttributes"/>
0283	<ResultStatus type="Enumeration" value="Success"/>
0284	<ResponsePayload>
0285	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0286	<Attribute>
0287	<AttributeName type="TextString" value="Digest"/>
0288	<AttributeValue>
0289	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0290	<DigestValue type="ByteString"
	value="314b223505091db03325c638a6016cf7080d3b116eb3f4896b6d24d4ec2215f8"/>
0291	<KeyFormatType type="Enumeration" value="Raw"/>
0292	</AttributeValue>
0293	</Attribute>
0294	</ResponsePayload>
0295	</BatchItem>
0296	</ResponseMessage>
	# TIME 6

0297	<RequestMessage>
0298	<RequestHeader>
0299	<ProtocolVersion>
0300	<ProtocolVersionMajor type="Integer" value="1"/>
0301	<ProtocolVersionMinor type="Integer" value="1"/>
0302	</ProtocolVersion>
0303	<BatchCount type="Integer" value="1"/>
0304	</RequestHeader>
0305	<BatchItem>
0306	<Operation type="Enumeration" value="Get"/>
0307	<RequestPayload>
0308	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0309	<KeyFormatType type="Enumeration" value="Raw"/>
0310	</RequestPayload>
0311	</BatchItem>
0312	</RequestMessage>
0313	<ResponseMessage>
0314	<ResponseHeader>
0315	<ProtocolVersion>
0316	<ProtocolVersionMajor type="Integer" value="1"/>
0317	<ProtocolVersionMinor type="Integer" value="1"/>
0318	</ProtocolVersion>
0319	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0320	<BatchCount type="Integer" value="1"/>
0321	</ResponseHeader>
0322	<BatchItem>
0323	<Operation type="Enumeration" value="Get"/>
0324	<ResultStatus type="Enumeration" value="Success"/>
0325	<ResponsePayload>
0326	<ObjectType type="Enumeration" value="SymmetricKey"/>
0327	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0328	<SymmetricKey>
0329	<KeyBlock>
0330	<KeyFormatType type="Enumeration" value="Raw"/>
0331	<KeyValue>
0332	<KeyMaterial type="ByteString"
	value="c1a99ac4716d4ea787d40b449d7b816f0ce82772b463cbf3a042b3f8e81e7bb7"/>
0333	</KeyValue>
0334	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0335	<CryptographicLength type="Integer" value="256"/>
0336	</KeyBlock>
0337	</SymmetricKey>
0338	</ResponsePayload>
0339	</BatchItem>
0340	</ResponseMessage>
	# TIME 7
0341	<RequestMessage>
0342	<RequestHeader>
0343	<ProtocolVersion>
0344	<ProtocolVersionMajor type="Integer" value="1"/>
0345	<ProtocolVersionMinor type="Integer" value="1"/>
0346	</ProtocolVersion>
0347	<BatchCount type="Integer" value="1"/>
0348	</RequestHeader>

0349	<BatchItem>
0350	<Operation type="Enumeration" value="Destroy"/>
0351	<RequestPayload>
0352	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0353	</RequestPayload>
0354	</BatchItem>
0355	</RequestMessage>
0356	<ResponseMessage>
0357	<ResponseHeader>
0358	<ProtocolVersion>
0359	<ProtocolVersionMajor type="Integer" value="1"/>
0360	<ProtocolVersionMinor type="Integer" value="1"/>
0361	</ProtocolVersion>
0362	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0363	<BatchCount type="Integer" value="1"/>
0364	</ResponseHeader>
0365	<BatchItem>
0366	<Operation type="Enumeration" value="Destroy"/>
0367	<ResultStatus type="Enumeration" value="Success"/>
0368	<ResponsePayload>
0369	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0370	</ResponsePayload>
0371	</BatchItem>
0372	</ResponseMessage>
	# TIME 8
0373	<RequestMessage>
0374	<RequestHeader>
0375	<ProtocolVersion>
0376	<ProtocolVersionMajor type="Integer" value="1"/>
0377	<ProtocolVersionMinor type="Integer" value="1"/>
0378	</ProtocolVersion>
0379	<BatchCount type="Integer" value="1"/>
0380	</RequestHeader>
0381	<BatchItem>
0382	<Operation type="Enumeration" value="Destroy"/>
0383	<RequestPayload>
0384	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0385	</RequestPayload>
0386	</BatchItem>
0387	</RequestMessage>
0388	<ResponseMessage>
0389	<ResponseHeader>
0390	<ProtocolVersion>
0391	<ProtocolVersionMajor type="Integer" value="1"/>
0392	<ProtocolVersionMinor type="Integer" value="1"/>
0393	</ProtocolVersion>
0394	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0395	<BatchCount type="Integer" value="1"/>
0396	</ResponseHeader>
0397	<BatchItem>
0398	<Operation type="Enumeration" value="Destroy"/>
0399	<ResultStatus type="Enumeration" value="Success"/>
0400	<ResponsePayload>

0401	<UniqueIdentifier type="TextString"
0402	value="\$UNIQUE_IDENTIFIER_1"/>
0403	</ResponsePayload>
0404	</BatchItem>
0405	</ResponseMessage>
# TIME 9	
0405	<RequestMessage>
0406	<RequestHeader>
0407	<ProtocolVersion>
0408	<ProtocolVersionMajor type="Integer" value="1"/>
0409	<ProtocolVersionMinor type="Integer" value="1"/>
0410	</ProtocolVersion>
0411	<BatchCount type="Integer" value="1"/>
0412	</RequestHeader>
0413	<BatchItem>
0414	<Operation type="Enumeration" value="Destroy"/>
0415	<RequestPayload>
0416	<UniqueIdentifier type="TextString"
0417	value="\$UNIQUE_IDENTIFIER_2"/>
0418	</RequestPayload>
0419	</BatchItem>
0420	</RequestMessage>
0421	<ResponseMessage>
0422	<ResponseHeader>
0423	<ProtocolVersion>
0424	<ProtocolVersionMajor type="Integer" value="1"/>
0425	<ProtocolVersionMinor type="Integer" value="1"/>
0426	</ProtocolVersion>
0427	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0428	<BatchCount type="Integer" value="1"/>
0429	</ResponseHeader>
0430	<BatchItem>
0431	<Operation type="Enumeration" value="Destroy"/>
0432	<ResultStatus type="Enumeration" value="Success"/>
0433	<ResponsePayload>
0434	<UniqueIdentifier type="TextString"
0435	value="\$UNIQUE_IDENTIFIER_2"/>
0436	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>

621

622 2.2.36 TC-182-11 - Digests of RSA Private Keys

623 Exercise the Digest attribute by registering two RSA private keys with the same key material but
624 using different Key Format Type. The Digest Value for the key with the Key Format Type set to
625 Transparent RSA Private Key is calculated on the TTLV-encoded Key Material structure, whereas
626 the Digest Value for the key registered in the PKCS_1 Key Format Type is calculated on the Key
627 Material Byte String. The server calculates the value of the mandatory Digest attribute instance
628 using the Key Format Type used by the client when registering the keys.

629 Note: This test case assumes a server that does not compute any additional Digest attributes
630 using another Hashing Algorithm and/or Key Format Type. A server is permitted to provide
631 multiple Digest attributes.

```
# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="1"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="Register"/>
0011     <RequestPayload>
0012       <ObjectType type="Enumeration" value="PrivateKey"/>
0013       <TemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0016           <AttributeValue type="Enumeration" value="RSA"/>
0017         </Attribute>
0018         <Attribute>
0019           <AttributeName type="TextString" value="Cryptographic
Length"/>
0020           <AttributeValue type="Integer" value="2048"/>
0021         </Attribute>
0022         <Attribute>
0023           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0024           <AttributeValue type="Integer" value="Sign"/>
0025         </Attribute>
0026         <Attribute>
0027           <AttributeName type="TextString" value="x-ID"/>
0028           <AttributeValue type="TextString" value="TC-182-11-
prikey1"/>
0029         </Attribute>
0030       </TemplateAttribute>
0031       <PrivateKey>
0032         <KeyBlock>
0033           <KeyFormatType type="Enumeration" value="PKCS_1"/>
0034           <KeyValue>
0035             <KeyMaterial type="ByteString"
value="308204a50201000282010100ab7f161c0042496ccd6c6d4dad9199734353
57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483
46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa
2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650
89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c
795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f
91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281
5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050
203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a
7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f
a74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b
2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0
e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a
a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e
3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78
965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8
c3cdc2464744a793713dafb9f1dbc799ff96423fecdc3ba794286bce920f4b5c183f
```

	99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967 4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064 b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e 59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4 990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766 b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab 7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0 e94adlee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa elebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2 7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eae9a922fd75d5b16b1a5 61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a72 6a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171 666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520 a2cea35800ad2724led360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a 1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d34941 7e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f812 9c32341a8b44f"/>
0036	</KeyValue>
0037	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0038	<CryptographicLength type="Integer" value="2048"/>
0039	</KeyBlock>
0040	</PrivateKey>
0041	</RequestPayload>
0042	</BatchItem>
0043	</RequestMessage>
0044	<ResponseMessage>
0045	<ResponseHeader>
0046	<ProtocolVersion>
0047	<ProtocolVersionMajor type="Integer" value="1"/>
0048	<ProtocolVersionMinor type="Integer" value="1"/>
0049	</ProtocolVersion>
0050	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0051	<BatchCount type="Integer" value="1"/>
0052	</ResponseHeader>
0053	<BatchItem>
0054	<Operation type="Enumeration" value="Register"/>
0055	<ResultStatus type="Enumeration" value="Success"/>
0056	<ResponsePayload>
0057	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0058	</ResponsePayload>
0059	</BatchItem>
0060	</ResponseMessage>
	# TIME 1
0061	<RequestMessage>
0062	<RequestHeader>
0063	<ProtocolVersion>
0064	<ProtocolVersionMajor type="Integer" value="1"/>
0065	<ProtocolVersionMinor type="Integer" value="1"/>
0066	</ProtocolVersion>
0067	<BatchCount type="Integer" value="1"/>
0068	</RequestHeader>
0069	<BatchItem>
0070	<Operation type="Enumeration" value="GetAttributes"/>
0071	<RequestPayload>

0072	<UniqueIdentifier type="TextString"
0073	value="\$UNIQUE_IDENTIFIER_0"/>
0074	<AttributeName type="TextString" value="Digest"/>
0075	</RequestPayload>
0076	</BatchItem>
0077	</RequestMessage>
0077	<ResponseMessage>
0078	<ResponseHeader>
0079	<ProtocolVersion>
0080	<ProtocolVersionMajor type="Integer" value="1"/>
0081	<ProtocolVersionMinor type="Integer" value="1"/>
0082	</ProtocolVersion>
0083	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0084	<BatchCount type="Integer" value="1"/>
0085	</ResponseHeader>
0086	<BatchItem>
0087	<Operation type="Enumeration" value="GetAttributes"/>
0088	<ResultStatus type="Enumeration" value="Success"/>
0089	<ResponsePayload>
0090	<UniqueIdentifier type="TextString"
0091	value="\$UNIQUE_IDENTIFIER_0"/>
0092	<Attribute>
0093	<AttributeName type="TextString" value="Digest"/>
0094	<AttributeValue>
0095	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0096	<DigestValue type="ByteString"
0097	value="11110a01ed4589d9987c9ad60368e2b762f2b20c00946e1932c1605a18172f55"/>
0098	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0099	</Attribute>
0100	</ResponsePayload>
0101	</BatchItem>
0102	</ResponseMessage>
0102	# TIME 2
0103	<RequestMessage>
0104	<RequestHeader>
0105	<ProtocolVersion>
0106	<ProtocolVersionMajor type="Integer" value="1"/>
0107	<ProtocolVersionMinor type="Integer" value="1"/>
0108	</ProtocolVersion>
0109	<BatchCount type="Integer" value="1"/>
0110	</RequestHeader>
0111	<BatchItem>
0112	<Operation type="Enumeration" value="Register"/>
0113	<RequestPayload>
0114	<ObjectType type="Enumeration" value="PrivateKey"/>
0115	<TemplateAttribute>
0116	<Attribute>
0117	<AttributeName type="TextString" value="Cryptographic"
0118	Algorithm"/>
0119	<AttributeValue type="Enumeration" value="RSA"/>
0120	</Attribute>
0121	<Attribute>
0122	<AttributeName type="TextString" value="Cryptographic"
0123	Length"/>
0124	<AttributeValue type="Integer" value="2048"/>

0122	</Attribute>
0123	<Attribute>
0124	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0125	<AttributeValue type="Integer" value="Sign"/>
0126	</Attribute>
0127	<Attribute>
0128	<AttributeName type="TextString" value="x-ID"/>
0129	<AttributeValue type="TextString" value="TC-182-11-prikey2"/>
0130	</Attribute>
0131	</TemplateAttribute>
0132	<PrivateKey>
0133	<KeyBlock>
0134	<KeyFormatType type="Enumeration" value="TransparentRSAPrivateKey"/>
0135	<KeyValue>
0136	<KeyMaterial>
0137	<Modulus type="BigInteger" value="0000000000000000ab7f161c0042496ccd6c6d4dadb919973435357776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f98135b1c67b701675abdbcd7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f605"/>
0138	<PrivateExponent type="BigInteger" value="3b12455d53c1816516c518493f6398aafa72b17dfa894db888a7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618fa74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0aa49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf29"/>
0139	<PublicExponent type="BigInteger" value="000000000010001"/>
0140	<P type="BigInteger" value="0000000000000000d5c69c8c3cdc2464744a793713dafb9f1dbc799ff96423fecdc3ba794286bce920f4b5c183f99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d5659674c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04cec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b"/>
0141	<Q type="BigInteger" value="0000000000000000cd5ea7702789064b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766b2bb9c985109974141b44d37e1e319820a55f"/>
0142	<PrimeExponentP type="BigInteger" value="0000000000000000b2871237bf9fad38c3316ab7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0e94adlee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920dbe22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aae1ebee3938f87c2707e178c739f9f"/>
0143	<PrimeExponentQ type="BigInteger"

0144	<pre> value="00000000000000009690bed14b2afaa26d986d592231ee27d71d49065bd2b a1f78157e20229881fd9d23227d0f8479eae9a922fd75d5b16b1a561fa6680b040ca 0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a726a1d90260e4f10 84f518234dcd3fe770b9520215bd543bb6a4117718754676a34171666a79f26e79c1 49c5aa1"/> <CRTCoefficient type="BigInteger" value="0000000000000000a0c985a0a0a791a659f99731134c44f37b2e520a2cea3 5800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a1cac91 011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d349417e1f0c 9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f8129c3234 1a8b44f"/> </KeyMaterial> </KeyValue> <CryptographicAlgorithm type="Enumeration" value="RSA"/> <CryptographicLength type="Integer" value="2048"/> </KeyBlock> </PrivateKey> </RequestPayload> </BatchItem> </RequestMessage> </pre>
0154 0155 0156 0157 0158 0159 0160 0161 0162 0163 0164 0165 0166 0167 0168 0169 0170	<pre> <ResponseMessage> <ResponseHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="1"/> </ProtocolVersion> <TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/> <BatchCount type="Integer" value="1"/> </ResponseHeader> <BatchItem> <Operation type="Enumeration" value="Register"/> <ResultStatus type="Enumeration" value="Success"/> <ResponsePayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> </ResponsePayload> </BatchItem> </ResponseMessage> </pre>
0171 0172 0173 0174 0175 0176 0177 0178 0179 0180 0181 0182 0183 0184 0185 0186	<pre> # TIME 3 <RequestMessage> <RequestHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="1"/> </ProtocolVersion> <BatchCount type="Integer" value="1"/> </RequestHeader> <BatchItem> <Operation type="Enumeration" value="GetAttributes"/> <RequestPayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> <AttributeName type="TextString" value="Digest"/> </RequestPayload> </BatchItem> </RequestMessage> </pre>

0187	<ResponseMessage>
0188	<ResponseHeader>
0189	<ProtocolVersion>
0190	<ProtocolVersionMajor type="Integer" value="1"/>
0191	<ProtocolVersionMinor type="Integer" value="1"/>
0192	</ProtocolVersion>
0193	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0194	<BatchCount type="Integer" value="1"/>
0195	</ResponseHeader>
0196	<BatchItem>
0197	<Operation type="Enumeration" value="GetAttributes"/>
0198	<ResultStatus type="Enumeration" value="Success"/>
0199	<ResponsePayload>
0200	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0201	<Attribute>
0202	<AttributeName type="TextString" value="Digest"/>
0203	<AttributeValue>
0204	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0205	<DigestValue type="ByteString"
	value="d73bbc51e83332935f912dbfc35c5efc3b7bf8021835ba86b8da4181f74244ac"/>
0206	<KeyFormatType type="Enumeration"
	value="TransparentRSAPrivateKey"/>
0207	</AttributeValue>
0208	</Attribute>
0209	</ResponsePayload>
0210	</BatchItem>
0211	</ResponseMessage>
	# TIME 4
0212	<RequestMessage>
0213	<RequestHeader>
0214	<ProtocolVersion>
0215	<ProtocolVersionMajor type="Integer" value="1"/>
0216	<ProtocolVersionMinor type="Integer" value="1"/>
0217	</ProtocolVersion>
0218	<BatchCount type="Integer" value="1"/>
0219	</RequestHeader>
0220	<BatchItem>
0221	<Operation type="Enumeration" value="Destroy"/>
0222	<RequestPayload>
0223	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0224	</RequestPayload>
0225	</BatchItem>
0226	</RequestMessage>
0227	<ResponseMessage>
0228	<ResponseHeader>
0229	<ProtocolVersion>
0230	<ProtocolVersionMajor type="Integer" value="1"/>
0231	<ProtocolVersionMinor type="Integer" value="1"/>
0232	</ProtocolVersion>
0233	<TimeStamp type="DateTime" value="2012-04-27T08:14:46+00:00"/>
0234	<BatchCount type="Integer" value="1"/>
0235	</ResponseHeader>
0236	<BatchItem>
0237	<Operation type="Enumeration" value="Destroy"/>

0238	<ResultStatus type="Enumeration" value="Success"/>
0239	<ResponsePayload>
0240	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0241	</ResponsePayload>
0242	</BatchItem>
0243	</ResponseMessage>
# TIME 5	
0244	<RequestMessage>
0245	<RequestHeader>
0246	<ProtocolVersion>
0247	<ProtocolVersionMajor type="Integer" value="1"/>
0248	<ProtocolVersionMinor type="Integer" value="1"/>
0249	</ProtocolVersion>
0250	<BatchCount type="Integer" value="1"/>
0251	</RequestHeader>
0252	<BatchItem>
0253	<Operation type="Enumeration" value="Destroy"/>
0254	<RequestPayload>
0255	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0256	</RequestPayload>
0257	</BatchItem>
0258	</RequestMessage>
0259	<ResponseMessage>
0260	<ResponseHeader>
0261	<ProtocolVersion>
0262	<ProtocolVersionMajor type="Integer" value="1"/>
0263	<ProtocolVersionMinor type="Integer" value="1"/>
0264	</ProtocolVersion>
0265	<TimeStamp type="DateTime" value="2012-04-27T08:14:46+00:00"/>
0266	<BatchCount type="Integer" value="1"/>
0267	</ResponseHeader>
0268	<BatchItem>
0269	<Operation type="Enumeration" value="Destroy"/>
0270	<ResultStatus type="Enumeration" value="Success"/>
0271	<ResponsePayload>
0272	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0273	</ResponsePayload>
0274	</BatchItem>
0275	</ResponseMessage>

632

633 2.2.37 TC-NP-1-11 - Put

634 In this test case the client issues a Create request, whereby the server creates a new symmetric
635 key and returns the Unique Identifier. To clean up, the client then performs a Destroy operation
636 to destroy the key.

637 The server sends Put messages to the client via a separate channel.

638

	# TIME 0
	# [Client-to-Server]

0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Length"/>
0022	<AttributeValue type="Integer" value="128"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Cryptographic
0026	Usage Mask"/>
0027	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="x-ID"/>
0031	<AttributeValue type="TextString" value="TC-NP-1-11"/>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	# [Client-to-Server]
0038	<ResponseMessage>
0039	<ResponseHeader>
0040	<ProtocolVersion>
0041	<ProtocolVersionMajor type="Integer" value="1"/>
0042	<ProtocolVersionMinor type="Integer" value="1"/>
0043	</ProtocolVersion>
0044	<TimeStamp type="DateTime" value="2013-06-26T05:13:47+00:00"/>
0045	<BatchCount type="Integer" value="1"/>
0046	</ResponseHeader>
0047	<BatchItem>
0048	<Operation type="Enumeration" value="Create"/>
0049	<ResultStatus type="Enumeration" value="Success"/>
0050	<ResponsePayload>
0051	<ObjectType type="Enumeration" value="SymmetricKey"/>
0052	<UniqueIdentifier type="TextString"
0053	value="\$UNIQUE_IDENTIFIER_0"/>
0054	</ResponsePayload>
0055	</BatchItem>
0056	</ResponseMessage>
0057	# TIME 1

```

0052 # [Server-to-Client]
0053 <RequestMessage>
0054   <RequestHeader>
0055     <ProtocolVersion>
0056       <ProtocolVersionMajor type="Integer" value="1"/>
0057       <ProtocolVersionMinor type="Integer" value="1"/>
0058     </ProtocolVersion>
0059     <BatchCount type="Integer" value="1"/>
0060   </RequestHeader>
0061   <BatchItem>
0062     <Operation type="Enumeration" value="Put"/>
0063     <RequestPayload>
0064       <UniqueIdentifier type="TextString"
0065       value="$UNIQUE_IDENTIFIER_0"/>
0066       <PutFunction type="Enumeration" value="New"/>
0067       <SymmetricKey>
0068         <KeyBlock>
0069           <KeyFormatType type="Enumeration" value="Raw"/>
0070           <KeyValue>
0071             <KeyMaterial type="ByteString"
0072             value="7546ef6cd37c49806824984477987dle"/>
0073           </KeyValue>
0074           <CryptographicAlgorithm type="Enumeration" value="AES"/>
0075           <CryptographicLength type="Integer" value="128"/>
0076         </KeyBlock>
0077       </SymmetricKey>
0078       <Attribute>
0079         <AttributeName type="TextString" value="x-ID"/>
0080         <AttributeValue type="TextString" value="TC-NP-1-11"/>
0081       </Attribute>
0082       <Attribute>
0083         <AttributeName type="TextString" value="Unique Identifier"/>
0084         <AttributeValue type="TextString"
0085         value="$UNIQUE_IDENTIFIER_0"/>
0086       </Attribute>
0087       <Attribute>
0088         <AttributeName type="TextString" value="Object Type"/>
0089         <AttributeValue type="Enumeration" value="SymmetricKey"/>
0090       </Attribute>
0091       <Attribute>
0092         <AttributeName type="TextString" value="Cryptographic
0093         Algorithm"/>
0094         <AttributeValue type="Enumeration" value="AES"/>
0095       </Attribute>
0096       <Attribute>
0097         <AttributeName type="TextString" value="Cryptographic
0098         Length"/>
0099         <AttributeValue type="Integer" value="128"/>
0100       </Attribute>
0101       <Attribute>
0102         <AttributeName type="TextString" value="Cryptographic Usage
0103         Mask"/>
0104         <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0105       </Attribute>
0106       <Attribute>
0107         <AttributeName type="TextString" value="Digest"/>
0108         <AttributeValue>

```

0102	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0103	<DigestValue type="ByteString"
	value="7549ecda2cd1569974c3748f223fbc947ce9cabce581497522e4b75e9d6ed
	e81"/>
0104	<KeyFormatType type="Enumeration" value="Raw"/>
0105	</AttributeValue>
0106	</Attribute>
0107	<Attribute>
0108	<AttributeName type="TextString" value="Fresh"/>
0109	<AttributeValue type="Boolean" value="true"/>
0110	</Attribute>
0111	<Attribute>
0112	<AttributeName type="TextString" value="Initial Date"/>
0113	<AttributeValue type="DateTime" value="2013-06-
	26T05:13:48+00:00"/>
0114	</Attribute>
0115	<Attribute>
0116	<AttributeName type="TextString" value="Last Change Date"/>
0117	<AttributeValue type="DateTime" value="2013-06-
	26T05:13:48+00:00"/>
0118	</Attribute>
0119	<Attribute>
0120	<AttributeName type="TextString" value="Lease Time"/>
0121	<AttributeValue type="Interval" value="3600"/>
0122	</Attribute>
0123	<Attribute>
0124	<AttributeName type="TextString" value="State"/>
0125	<AttributeValue type="Enumeration" value="PreActive"/>
0126	</Attribute>
0127	</RequestPayload>
0128	</BatchItem>
0129	</RequestMessage>
	# [Server-to-Client]
0130	<ResponseMessage>
0131	<ResponseHeader>
0132	<ProtocolVersion>
0133	<ProtocolVersionMajor type="Integer" value="1"/>
0134	<ProtocolVersionMinor type="Integer" value="1"/>
0135	</ProtocolVersion>
0136	<TimeStamp type="DateTime" value="2013-06-26T05:13:48+00:00"/>
0137	<BatchCount type="Integer" value="1"/>
0138	</ResponseHeader>
0139	<BatchItem>
0140	<Operation type="Enumeration" value="Put"/>
0141	<ResultStatus type="Enumeration" value="Success"/>
0142	<ResponsePayload>
0143	</ResponsePayload>
0144	</BatchItem>
0145	</ResponseMessage>
	# TIME 2
	# [Client-to-Server]
0146	<RequestMessage>
0147	<RequestHeader>
0148	<ProtocolVersion>
0149	<ProtocolVersionMajor type="Integer" value="1"/>
0150	<ProtocolVersionMinor type="Integer" value="1"/>
0151	</ProtocolVersion>

0152	<BatchCount type="Integer" value="1"/>
0153	</RequestHeader>
0154	<BatchItem>
0155	<Operation type="Enumeration" value="Destroy"/>
0156	<RequestPayload>
0157	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0158	</RequestPayload>
0159	</BatchItem>
0160	</RequestMessage>
	# [Client-to-Server]
0161	<ResponseMessage>
0162	<ResponseHeader>
0163	<ProtocolVersion>
0164	<ProtocolVersionMajor type="Integer" value="1"/>
0165	<ProtocolVersionMinor type="Integer" value="1"/>
0166	</ProtocolVersion>
0167	<TimeStamp type="DateTime" value="2013-06-26T05:13:48+00:00"/>
0168	<BatchCount type="Integer" value="1"/>
0169	</ResponseHeader>
0170	<BatchItem>
0171	<Operation type="Enumeration" value="Destroy"/>
0172	<ResultStatus type="Enumeration" value="Success"/>
0173	<ResponsePayload>
0174	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0175	</ResponsePayload>
0176	</BatchItem>
0177	</ResponseMessage>

639

640 2.2.38 TC-NP-2-11 - Notify & Put

641 This test case tests the import of key using the Register operation. To validate that the
642 registered key is treated the same as a locally created key, an attribute is added to the key and
643 then modified. Finally, the key is destroyed.

644 The server sends Notify and Put messages to the client via a separate channel.

	# TIME 0
	# [Client-to-Server]
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic

0016	Usage Mask"/>
0017	<AttributeValue type="Integer" value="Encrypt"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="x-ID"/>
0021	<AttributeValue type="TextString" value="TC-NP-2-11"/>
0022	</Attribute>
0023	</TemplateAttribute>
0024	<SymmetricKey>
0025	<KeyBlock>
0026	<KeyFormatType type="Enumeration" value="Raw"/>
0027	<KeyValue>
0028	<KeyMaterial type="ByteString"
0029	value="1122456789abcdef0123456789abcdef"/>
0030	</KeyValue>
0031	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0032	<CryptographicLength type="Integer" value="128"/>
0033	</KeyBlock>
0034	</SymmetricKey>
0035	</RequestPayload>
0036	</BatchItem>
0037	</RequestMessage>
0038	# [Client-to-Server]
0039	<ResponseMessage>
0040	<ResponseHeader>
0041	<ProtocolVersion>
0042	<ProtocolVersionMajor type="Integer" value="1"/>
0043	<ProtocolVersionMinor type="Integer" value="1"/>
0044	</ProtocolVersion>
0045	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0046	<BatchCount type="Integer" value="1"/>
0047	</ResponseHeader>
0048	<BatchItem>
0049	<Operation type="Enumeration" value="Register"/>
0050	<ResultStatus type="Enumeration" value="Success"/>
0051	<ResponsePayload>
0052	<UniqueIdentifier type="TextString"
0053	value="\$UNIQUE_IDENTIFIER_0"/>
0054	</ResponsePayload>
0055	</BatchItem>
0056	</ResponseMessage>
0057	# TIME 1
0058	# [Server-to-Client]
0059	<RequestMessage>
0060	<RequestHeader>
0061	<ProtocolVersion>
0062	<ProtocolVersionMajor type="Integer" value="1"/>
0063	<ProtocolVersionMinor type="Integer" value="1"/>
0064	</ProtocolVersion>
0065	<BatchCount type="Integer" value="1"/>
0066	</RequestHeader>
0067	<BatchItem>
0068	<Operation type="Enumeration" value="Put"/>
0069	<RequestPayload>
0070	<UniqueIdentifier type="TextString"
0071	value="\$UNIQUE_IDENTIFIER_0"/>
0072	<PutFunction type="Enumeration" value="New"/>

```

0066     <SymmetricKey>
0067         <KeyBlock>
0068             <KeyFormatType type="Enumeration" value="Raw"/>
0069             <KeyValue>
0070                 <KeyMaterial type="ByteString"
value="1122456789abcdef0123456789abcdef"/>
0071             </KeyValue>
0072             <CryptographicAlgorithm type="Enumeration" value="AES"/>
0073             <CryptographicLength type="Integer" value="128"/>
0074         </KeyBlock>
0075     </SymmetricKey>
0076     <Attribute>
0077         <AttributeName type="TextString" value="x-ID"/>
0078         <AttributeValue type="TextString" value="TC-NP-2-11"/>
0079     </Attribute>
0080     <Attribute>
0081         <AttributeName type="TextString" value="Unique Identifier"/>
0082         <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0083     </Attribute>
0084     <Attribute>
0085         <AttributeName type="TextString" value="Object Type"/>
0086         <AttributeValue type="Enumeration" value="SymmetricKey"/>
0087     </Attribute>
0088     <Attribute>
0089         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0090         <AttributeValue type="Enumeration" value="AES"/>
0091     </Attribute>
0092     <Attribute>
0093         <AttributeName type="TextString" value="Cryptographic
Length"/>
0094         <AttributeValue type="Integer" value="128"/>
0095     </Attribute>
0096     <Attribute>
0097         <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0098         <AttributeValue type="Integer" value="Encrypt"/>
0099     </Attribute>
0100     <Attribute>
0101         <AttributeName type="TextString" value="Digest"/>
0102         <AttributeValue>
0103             <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0104             <DigestValue type="ByteString"
value="47c01d3851ce2f254d18928526b6126de30cef9a34a4cfbd4648ec3ed21a9
e86"/>
0105         <KeyFormatType type="Enumeration" value="Raw"/>
0106     </AttributeValue>
0107 </Attribute>
0108 <Attribute>
0109     <AttributeName type="TextString" value="Fresh"/>
0110     <AttributeValue type="Boolean" value="true"/>
0111 </Attribute>
0112 <Attribute>
0113     <AttributeName type="TextString" value="Initial Date"/>
0114     <AttributeValue type="DateTime" value="2013-06-
26T05:54:18+00:00"/>

```


0115	</Attribute>
0116	<Attribute>
0117	<AttributeName type="TextString" value="Last Change Date"/>
0118	<AttributeValue type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0119	</Attribute>
0120	<Attribute>
0121	<AttributeName type="TextString" value="Lease Time"/>
0122	<AttributeValue type="Interval" value="3600"/>
0123	</Attribute>
0124	<Attribute>
0125	<AttributeName type="TextString" value="State"/>
0126	<AttributeValue type="Enumeration" value="PreActive"/>
0127	</Attribute>
0128	</RequestPayload>
0129	</BatchItem>
0130	</RequestMessage>
# [Server-to-Client]	
0131	<ResponseMessage>
0132	<ResponseHeader>
0133	<ProtocolVersion>
0134	<ProtocolVersionMajor type="Integer" value="1"/>
0135	<ProtocolVersionMinor type="Integer" value="1"/>
0136	</ProtocolVersion>
0137	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0138	<BatchCount type="Integer" value="1"/>
0139	</ResponseHeader>
0140	<BatchItem>
0141	<Operation type="Enumeration" value="Put"/>
0142	<ResultStatus type="Enumeration" value="Success"/>
0143	<ResponsePayload>
0144	</ResponsePayload>
0145	</BatchItem>
0146	</ResponseMessage>
# TIME 2	
# [Client-to-Server]	
0147	<RequestMessage>
0148	<RequestHeader>
0149	<ProtocolVersion>
0150	<ProtocolVersionMajor type="Integer" value="1"/>
0151	<ProtocolVersionMinor type="Integer" value="1"/>
0152	</ProtocolVersion>
0153	<BatchCount type="Integer" value="1"/>
0154	</RequestHeader>
0155	<BatchItem>
0156	<Operation type="Enumeration" value="AddAttribute"/>
0157	<RequestPayload>
0158	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0159	<Attribute>
0160	<AttributeName type="TextString" value="x-provider"/>
0161	<AttributeValue type="TextString" value="unknown"/>
0162	</Attribute>
0163	</RequestPayload>
0164	</BatchItem>
0165	</RequestMessage>

0166	# [Client-to-Server]
0167	<ResponseMessage>
0168	<ResponseHeader>
0169	<ProtocolVersion>
0170	<ProtocolVersionMajor type="Integer" value="1"/>
0171	<ProtocolVersionMinor type="Integer" value="1"/>
0172	</ProtocolVersion>
0173	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0174	<BatchCount type="Integer" value="1"/>
0175	</ResponseHeader>
0176	<BatchItem>
0177	<Operation type="Enumeration" value="AddAttribute"/>
0178	<ResultStatus type="Enumeration" value="Success"/>
0179	<ResponsePayload>
0180	<UniqueIdentifier type="TextString"
0181	value="\$UNIQUE_IDENTIFIER_0"/>
0182	<Attribute>
0183	<AttributeName type="TextString" value="x-provider"/>
0184	<AttributeValue type="TextString" value="unknown"/>
0185	</Attribute>
0186	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>
	# TIME 3
	# [Server-to-Client]
0187	<RequestMessage>
0188	<RequestHeader>
0189	<ProtocolVersion>
0190	<ProtocolVersionMajor type="Integer" value="1"/>
0191	<ProtocolVersionMinor type="Integer" value="1"/>
0192	</ProtocolVersion>
0193	<BatchCount type="Integer" value="1"/>
0194	</RequestHeader>
0195	<BatchItem>
0196	<Operation type="Enumeration" value="Notify"/>
0197	<RequestPayload>
0198	<UniqueIdentifier type="TextString"
0199	value="\$UNIQUE_IDENTIFIER_0"/>
0200	<Attribute>
0201	<AttributeName type="TextString" value="x-provider"/>
0202	<AttributeValue type="TextString" value="unknown"/>
0203	</Attribute>
0204	<Attribute>
0205	<AttributeName type="TextString" value="Last Change Date"/>
0206	<AttributeValue type="DateTime" value="2013-06-
0207	26T05:54:18+00:00"/>
0208	</Attribute>
0209	</RequestPayload>
	</BatchItem>
	</RequestMessage>
	# [Server-to-Client]
0210	<ResponseMessage>
0211	<ResponseHeader>
0212	<ProtocolVersion>
0213	<ProtocolVersionMajor type="Integer" value="1"/>
0214	<ProtocolVersionMinor type="Integer" value="1"/>
0215	</ProtocolVersion>

0216	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0217	<BatchCount type="Integer" value="1"/>
0218	</ResponseHeader>
0219	<BatchItem>
0220	<Operation type="Enumeration" value="Notify"/>
0221	<ResultStatus type="Enumeration" value="Success"/>
0222	<ResponsePayload>
0223	</ResponsePayload>
0224	</BatchItem>
0225	</ResponseMessage>
# TIME 4	
# [Client-to-Server]	
0226	<RequestMessage>
0227	<RequestHeader>
0228	<ProtocolVersion>
0229	<ProtocolVersionMajor type="Integer" value="1"/>
0230	<ProtocolVersionMinor type="Integer" value="1"/>
0231	</ProtocolVersion>
0232	<BatchCount type="Integer" value="1"/>
0233	</RequestHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="ModifyAttribute"/>
0236	<RequestPayload>
0237	<UniqueIdentifier type="TextString"
0238	value="\$UNIQUE_IDENTIFIER_0"/>
0239	<Attribute>
0240	<AttributeName type="TextString" value="x-provider"/>
0241	<AttributeValue type="TextString" value="third party"/>
0242	</Attribute>
0243	</RequestPayload>
0244	</BatchItem>
0245	</RequestMessage>
# [Client-to-Server]	
0246	<ResponseMessage>
0247	<ResponseHeader>
0248	<ProtocolVersion>
0249	<ProtocolVersionMajor type="Integer" value="1"/>
0250	<ProtocolVersionMinor type="Integer" value="1"/>
0251	</ProtocolVersion>
0252	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0253	<BatchCount type="Integer" value="1"/>
0254	</ResponseHeader>
0255	<BatchItem>
0256	<Operation type="Enumeration" value="ModifyAttribute"/>
0257	<ResultStatus type="Enumeration" value="Success"/>
0258	<ResponsePayload>
0259	<UniqueIdentifier type="TextString"
0260	value="\$UNIQUE_IDENTIFIER_0"/>
0261	<Attribute>
0262	<AttributeName type="TextString" value="x-provider"/>
0263	<AttributeValue type="TextString" value="third party"/>
0264	</Attribute>
0265	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>
	# TIME 5

0266	# [Server-to-Client]
0267	<RequestMessage>
0268	<RequestHeader>
0269	<ProtocolVersion>
0270	<ProtocolVersionMajor type="Integer" value="1"/>
0271	<ProtocolVersionMinor type="Integer" value="1"/>
0272	</ProtocolVersion>
0273	<BatchCount type="Integer" value="1"/>
0274	</RequestHeader>
0275	<BatchItem>
0276	<Operation type="Enumeration" value="Notify"/>
0277	<RequestPayload>
0278	<UniqueIdentifier type="TextString"
0279	value="\$UNIQUE_IDENTIFIER_0"/>
0280	<Attribute>
0281	<AttributeName type="TextString" value="x-provider"/>
0282	<AttributeValue type="TextString" value="third party"/>
0283	</Attribute>
0284	<Attribute>
0285	<AttributeName type="TextString" value="Last Change Date"/>
0286	<AttributeValue type="DateTime" value="2013-06-
0287	26T05:54:18+00:00"/>
0288	</Attribute>
0289	</RequestPayload>
0290	</BatchItem>
0291	</RequestMessage>
0292	# [Server-to-Client]
0293	<ResponseMessage>
0294	<ResponseHeader>
0295	<ProtocolVersion>
0296	<ProtocolVersionMajor type="Integer" value="1"/>
0297	<ProtocolVersionMinor type="Integer" value="1"/>
0298	</ProtocolVersion>
0299	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0300	<BatchCount type="Integer" value="1"/>
0301	</ResponseHeader>
0302	<BatchItem>
0303	<Operation type="Enumeration" value="Notify"/>
0304	<ResultStatus type="Enumeration" value="Success"/>
0305	<ResponsePayload>
0306	</ResponsePayload>
0307	</BatchItem>
0308	</ResponseMessage>
0309	# TIME 6
0310	# [Client-to-Server]
0311	<RequestMessage>
0312	<RequestHeader>
0313	<ProtocolVersion>
0314	<ProtocolVersionMajor type="Integer" value="1"/>
0315	<ProtocolVersionMinor type="Integer" value="1"/>
0316	</ProtocolVersion>
	<BatchCount type="Integer" value="1"/>
	</RequestHeader>
	<BatchItem>
	<Operation type="Enumeration" value="Destroy"/>
	<RequestPayload>
	<UniqueIdentifier type="TextString"

0317	value="\$UNIQUE_IDENTIFIER_0"/>
0318	</RequestPayload>
0319	</BatchItem>
	</RequestMessage>
0320	# [Client-to-Server]
0321	<ResponseMessage>
0322	<ResponseHeader>
0323	<ProtocolVersion>
0324	<ProtocolVersionMajor type="Integer" value="1"/>
0325	<ProtocolVersionMinor type="Integer" value="1"/>
0326	</ProtocolVersion>
0327	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0328	<BatchCount type="Integer" value="1"/>
0329	</ResponseHeader>
0330	<BatchItem>
0331	<Operation type="Enumeration" value="Destroy"/>
0332	<ResultStatus type="Enumeration" value="Success"/>
0333	<ResponsePayload>
0334	<UniqueIdentifier type="TextString"
0335	value="\$UNIQUE_IDENTIFIER_0"/>
0336	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>
0337	# TIME 7
0338	# [Server-to-Client]
0339	<RequestMessage>
0340	<RequestHeader>
0341	<ProtocolVersion>
0342	<ProtocolVersionMajor type="Integer" value="1"/>
0343	<ProtocolVersionMinor type="Integer" value="1"/>
0344	</ProtocolVersion>
0345	<BatchCount type="Integer" value="1"/>
0346	</RequestHeader>
0347	<BatchItem>
0348	<Operation type="Enumeration" value="Notify"/>
0349	<RequestPayload>
0350	<UniqueIdentifier type="TextString"
0351	value="\$UNIQUE_IDENTIFIER_0"/>
0352	<Attribute>
0353	<AttributeName type="TextString" value="Last Change Date"/>
0354	<AttributeValue type="DateTime" value="2013-06-
0355	26T05:54:18+00:00"/>
0356	</Attribute>
0357	<Attribute>
0358	<AttributeName type="TextString" value="State"/>
0359	<AttributeValue type="Enumeration" value="Destroyed"/>
	</Attribute>
	</RequestPayload>
	</BatchItem>
	</RequestMessage>
0360	# [Server-to-Client]
0361	<ResponseMessage>
0362	<ResponseHeader>
0363	<ProtocolVersion>
0364	<ProtocolVersionMajor type="Integer" value="1"/>
	<ProtocolVersionMinor type="Integer" value="1"/>

0365	</ProtocolVersion>
0366	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0367	<BatchCount type="Integer" value="1"/>
0368	</ResponseHeader>
0369	<BatchItem>
0370	<Operation type="Enumeration" value="Notify"/>
0371	<ResultStatus type="Enumeration" value="Success"/>
0372	<ResponsePayload>
0373	</ResponsePayload>
0374	</BatchItem>
0375	</ResponseMessage>

645

646 2.2.39 TC-ECC-1-11 - Register an ECC Key Pair

647 EC recommended curve is P-256 (secp256r1)

648 - Private Key format ECPrivateKey - <http://tools.ietf.org/html/rfc5915>

649 - Public Key format SubjectPublicKeyInfo - <http://tools.ietf.org/html/rfc5480>

650 Register a EC private key in the ECPrivateKey key format, then register the corresponding public
651 key, in X.509 (SubjectPublicKeyInfo) format, with the Link attribute pointing to the previously
652 registered private key. Then add the Link attribute to the private key, and perform Locate
653 operations to find the public and private keys using the Link attribute. Get both the private and
654 public keys in default format, then destroy both the private and the public key.

655

656 -----BEGIN EC PRIVATE KEY-----
657 MHcCAQEEIJEqDiCPXdc0sYUYR+RlnEWIsW2fO8GtpRDqLJadr570oAoGCCqGSM49
658 AwEHoUQDQgAes0Q5L7cqomf4bX2DfeHZbOlg/8Bc7vPx+ibYVGpkQvPBOX6Smq2N
659 yrJbKCYooc8AvvfLGKD16kRJOjCm0iOyWw==
660 -----END EC PRIVATE KEY-----
661
662 -----BEGIN PUBLIC KEY-----
663 MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAes0Q5L7cqomf4bX2DfeHZbOlg/8Bc
664 7vPx+ibYVGpkQvPBOX6Smq2NyrJbKCYooc8AvvfLGKD16kRJOjCm0iOyWw==
665 -----END PUBLIC KEY-----
666
667

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="PrivateKey"/>

0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Sign"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-ECC-1-11-prikey1"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<PrivateKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="ECPrivateKey"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString" value="30770201010420912a0e208f5dd734b1851847e4659c4588b16d9f3bclada510ea2c969daf9ef4a00a06082a8648ce3d030107a14403420004b344392fb72aa267f86d7d837delld96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aad8dcab25b282ca8alcf00bef7cb18a0f5ea44493a30a6d223b25b"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0030	<CryptographicLength type="Integer" value="256"/>
0031	</KeyBlock>
0032	</PrivateKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="1"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
0053	# TIME 1 <RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="1"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>

0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PublicKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0068	<AttributeValue type="Integer" value="Verify"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>
0073	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0075	</AttributeValue>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-ECC-1-11-pubkey1"/>
0080	</Attribute>
0081	</TemplateAttribute>
0082	<PublicKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="X_509"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString" value="3059301306072a8648ce3d020106082a8648ce3d03010703420004b344392fb72aa267f86d7d837de1d96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aad8dcab25b282ca8alc00bef7cb18a0f5ea44493a30a6d223b25b"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0089	<CryptographicLength type="Integer" value="256"/>
0090	</KeyBlock>
0091	</PublicKey>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="1"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0109	</ResponsePayload>
0110	</BatchItem>
0111	</ResponseMessage>

0112 0113 0114 0115 0116 0117 0118 0119 0120 0121 0122 0123 0124 0125 0126 0127 0128 0129 0130 0131 0132 0133	<pre> # TIME 2 <RequestMessage> <RequestHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="1"/> </ProtocolVersion> <BatchCount type="Integer" value="1"/> </RequestHeader> <BatchItem> <Operation type="Enumeration" value="AddAttribute"/> <RequestPayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/> <Attribute> <AttributeName type="TextString" value="Link"/> <AttributeValue> <LinkType type="Enumeration" value="PublicKeyLink"/> <LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> </AttributeValue> </Attribute> </RequestPayload> </BatchItem> </RequestMessage> </pre>
0134 0135 0136 0137 0138 0139 0140 0141 0142 0143 0144 0145 0146 0147 0148 0149 0150 0151 0152 0153 0154 0155 0156 0157	<pre> <ResponseMessage> <ResponseHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="1"/> </ProtocolVersion> <TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/> <BatchCount type="Integer" value="1"/> </ResponseHeader> <BatchItem> <Operation type="Enumeration" value="AddAttribute"/> <ResultStatus type="Enumeration" value="Success"/> <ResponsePayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/> <Attribute> <AttributeName type="TextString" value="Link"/> <AttributeValue> <LinkType type="Enumeration" value="PublicKeyLink"/> <LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> </AttributeValue> </Attribute> </ResponsePayload> </BatchItem> </ResponseMessage> </pre>
0158 0159 0160 0161 0162	<pre> # TIME 3 <RequestMessage> <RequestHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="1"/> </ProtocolVersion> </RequestHeader> </pre>

0163	</ProtocolVersion>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Locate"/>
0168	<RequestPayload>
0169	<Attribute>
0170	<AttributeName type="TextString" value="Object Type"/>
0171	<AttributeValue type="Enumeration" value="PublicKey"/>
0172	</Attribute>
0173	<Attribute>
0174	<AttributeName type="TextString" value="Link"/>
0175	<AttributeValue>
0176	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0177	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0178	</AttributeValue>
0179	</Attribute>
0180	</RequestPayload>
0181	</BatchItem>
0182	</RequestMessage>
0183	<ResponseMessage>
0184	<ResponseHeader>
0185	<ProtocolVersion>
0186	<ProtocolVersionMajor type="Integer" value="1"/>
0187	<ProtocolVersionMinor type="Integer" value="1"/>
0188	</ProtocolVersion>
0189	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0190	<BatchCount type="Integer" value="1"/>
0191	</ResponseHeader>
0192	<BatchItem>
0193	<Operation type="Enumeration" value="Locate"/>
0194	<ResultStatus type="Enumeration" value="Success"/>
0195	<ResponsePayload>
0196	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0197	</ResponsePayload>
0198	</BatchItem>
0199	</ResponseMessage>
	# TIME 4
0200	<RequestMessage>
0201	<RequestHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="1"/>
0205	</ProtocolVersion>
0206	<BatchCount type="Integer" value="1"/>
0207	</RequestHeader>
0208	<BatchItem>
0209	<Operation type="Enumeration" value="Locate"/>
0210	<RequestPayload>
0211	<Attribute>
0212	<AttributeName type="TextString" value="Object Type"/>
0213	<AttributeValue type="Enumeration" value="PrivateKey"/>
0214	</Attribute>
0215	<Attribute>
0216	<AttributeName type="TextString" value="Link"/>

0217	<AttributeValue>
0218	<LinkType type="Enumeration" value="PublicKeyLink"/>
0219	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0220	</AttributeValue>
0221	</Attribute>
0222	</RequestPayload>
0223	</BatchItem>
0224	</RequestMessage>
0225	<ResponseMessage>
0226	<ResponseHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="1"/>
0230	</ProtocolVersion>
0231	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0232	<BatchCount type="Integer" value="1"/>
0233	</ResponseHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="Locate"/>
0236	<ResultStatus type="Enumeration" value="Success"/>
0237	<ResponsePayload>
0238	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0239	</ResponsePayload>
0240	</BatchItem>
0241	</ResponseMessage>
	# TIME 5
0242	<RequestMessage>
0243	<RequestHeader>
0244	<ProtocolVersion>
0245	<ProtocolVersionMajor type="Integer" value="1"/>
0246	<ProtocolVersionMinor type="Integer" value="1"/>
0247	</ProtocolVersion>
0248	<BatchCount type="Integer" value="1"/>
0249	</RequestHeader>
0250	<BatchItem>
0251	<Operation type="Enumeration" value="Get"/>
0252	<RequestPayload>
0253	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0254	</RequestPayload>
0255	</BatchItem>
0256	</RequestMessage>
0257	<ResponseMessage>
0258	<ResponseHeader>
0259	<ProtocolVersion>
0260	<ProtocolVersionMajor type="Integer" value="1"/>
0261	<ProtocolVersionMinor type="Integer" value="1"/>
0262	</ProtocolVersion>
0263	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0264	<BatchCount type="Integer" value="1"/>
0265	</ResponseHeader>
0266	<BatchItem>
0267	<Operation type="Enumeration" value="Get"/>
0268	<ResultStatus type="Enumeration" value="Success"/>

0269	<ResponsePayload>
0270	<ObjectType type="Enumeration" value="PrivateKey"/>
0271	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0272	<PrivateKey>
0273	<KeyBlock>
0274	<KeyFormatType type="Enumeration" value="ECPrivateKey"/>
0275	<KeyValue>
0276	<KeyMaterial type="ByteString"
	value="30770201010420912a0e208f5dd734b1851847e4659c4588b16d9f3bclada
	510ea2c969daf9ef4a00a06082a8648ce3d030107a14403420004b344392fb72aa26
	7f86d7d837de1d96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aad8dcab25
	b282ca8alcf00bef7cb18a0f5ea44493a30a6d223b25b"/>
0277	</KeyValue>
0278	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0279	<CryptographicLength type="Integer" value="256"/>
0280	</KeyBlock>
0281	</PrivateKey>
0282	</ResponsePayload>
0283	</BatchItem>
0284	</ResponseMessage>
	# TIME 6
0285	<RequestMessage>
0286	<RequestHeader>
0287	<ProtocolVersion>
0288	<ProtocolVersionMajor type="Integer" value="1"/>
0289	<ProtocolVersionMinor type="Integer" value="1"/>
0290	</ProtocolVersion>
0291	<BatchCount type="Integer" value="1"/>
0292	</RequestHeader>
0293	<BatchItem>
0294	<Operation type="Enumeration" value="Get"/>
0295	<RequestPayload>
0296	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0297	</RequestPayload>
0298	</BatchItem>
0299	</RequestMessage>
0300	<ResponseMessage>
0301	<ResponseHeader>
0302	<ProtocolVersion>
0303	<ProtocolVersionMajor type="Integer" value="1"/>
0304	<ProtocolVersionMinor type="Integer" value="1"/>
0305	</ProtocolVersion>
0306	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0307	<BatchCount type="Integer" value="1"/>
0308	</ResponseHeader>
0309	<BatchItem>
0310	<Operation type="Enumeration" value="Get"/>
0311	<ResultStatus type="Enumeration" value="Success"/>
0312	<ResponsePayload>
0313	<ObjectType type="Enumeration" value="PublicKey"/>
0314	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0315	<PublicKey>
0316	<KeyBlock>
0317	<KeyFormatType type="Enumeration" value="X 509"/>

0318	<KeyValue>
0319	<KeyMaterial type="ByteString"
	value="3059301306072a8648ce3d020106082a8648ce3d03010703420004b344392fb72aa267f86d7d837deld96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aad8dcab25b282ca8a1cf00bef7cb18a0f5ea44493a30a6d223b25b"/>
0320	</KeyMaterial>
0321	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0322	<CryptographicLength type="Integer" value="256"/>
0323	</KeyBlock>
0324	</PublicKey>
0325	</ResponsePayload>
0326	</BatchItem>
0327	</ResponseMessage>
	# TIME 7
0328	<RequestMessage>
0329	<RequestHeader>
0330	<ProtocolVersion>
0331	<ProtocolVersionMajor type="Integer" value="1"/>
0332	<ProtocolVersionMinor type="Integer" value="1"/>
0333	</ProtocolVersion>
0334	<BatchCount type="Integer" value="1"/>
0335	</RequestHeader>
0336	<BatchItem>
0337	<Operation type="Enumeration" value="Destroy"/>
0338	<RequestPayload>
0339	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0340	</RequestPayload>
0341	</BatchItem>
0342	</RequestMessage>
0343	<ResponseMessage>
0344	<ResponseHeader>
0345	<ProtocolVersion>
0346	<ProtocolVersionMajor type="Integer" value="1"/>
0347	<ProtocolVersionMinor type="Integer" value="1"/>
0348	</ProtocolVersion>
0349	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0350	<BatchCount type="Integer" value="1"/>
0351	</ResponseHeader>
0352	<BatchItem>
0353	<Operation type="Enumeration" value="Destroy"/>
0354	<ResultStatus type="Enumeration" value="Success"/>
0355	<ResponsePayload>
0356	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0357	</ResponsePayload>
0358	</BatchItem>
0359	</ResponseMessage>
	# TIME 8
0360	<RequestMessage>
0361	<RequestHeader>
0362	<ProtocolVersion>
0363	<ProtocolVersionMajor type="Integer" value="1"/>
0364	<ProtocolVersionMinor type="Integer" value="1"/>
0365	</ProtocolVersion>
0366	<BatchCount type="Integer" value="1"/>

0367	</RequestHeader>
0368	<BatchItem>
0369	<Operation type="Enumeration" value="Destroy"/>
0370	<RequestPayload>
0371	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0372	</RequestPayload>
0373	</BatchItem>
0374	</RequestMessage>
0375	<ResponseMessage>
0376	<ResponseHeader>
0377	<ProtocolVersion>
0378	<ProtocolVersionMajor type="Integer" value="1"/>
0379	<ProtocolVersionMinor type="Integer" value="1"/>
0380	</ProtocolVersion>
0381	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0382	<BatchCount type="Integer" value="1"/>
0383	</ResponseHeader>
0384	<BatchItem>
0385	<Operation type="Enumeration" value="Destroy"/>
0386	<ResultStatus type="Enumeration" value="Success"/>
0387	<ResponsePayload>
0388	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0389	</ResponsePayload>
0390	</BatchItem>
0391	</ResponseMessage>

668

669 2.2.40 TC-ECC-2-11 - Register an ECC Key Pair in PKCS8 Format

670 EC recommended curve is P-256 (secp256r1)

671 - Public Key format SubjectPublicKeyInfo - <http://tools.ietf.org/html/rfc5480>

672 Register a EC private key in PKCS8 key format (with passphrase 'secret' using pbeWithSHAAnd3-
673 KeyTripleDES-CBC), then register the corresponding public key, in X.509 (SubjectPublicKeyInfo)
674 format, with the Link attribute pointing to the previously registered private key. Then add the
675 Link attribute to the private key, and perform Locate operations to find the public and private
676 keys using the Link attribute. Get both the private and public keys in default format, then
677 destroy both the private and the public key.

678

679 -----BEGIN ENCRYPTED PRIVATE KEY-----
680 MIGxMBwGCIqGSib3DQEMAQMwDgQIqCAF0cAFxb4CAggABIGQkUySNQqsjKPKt19y
681 g/n+qhaBSsolURUH4PBYPVpWVUNzqKQhz0MD8/gfBSz1DOU9s7mC97LVgWaEqJTad
682 sOgPsJL3Z4IUuNTWNOMLZtY3jDz4z4grmyYM2c/aJj9eYVu0Ufp6n1lCsdU6HFpn
683 urzWFArK+Yt+zpokG+raOoo08kIz59Fm30ziZPZF4G74GMM
684 -----END ENCRYPTED PRIVATE KEY-----
685
686 -----BEGIN PUBLIC KEY-----
687 MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEs0Q5L7cqomf4bX2DfeHZbOlG/8Bc
688 7vPx+ibYVGpkQvPBOX6Smq2NyrJbKCYooc8AvvfLGKD16kRJOjCm0iOyWw==
689 -----END PUBLIC KEY-----

690

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="PrivateKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Sign"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-ECC-2-11-prikey1"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<PrivateKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="PKCS_8"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString" value="3081b1301c060a2a864886f70d010c0103300e04082f2656a33657313902020800048190eadf76e9cee21053b01c53e175b0e8c4d627c17dalb2df47d8cfb35a0d7252a9a6488660d61235be735178d0ca8548871567c22803d8f6f6009f05c26429c83ab72d0f2e7e7870befc3ec746f52d0eccafe34b72a791e9535b34f584b96dc124034e8a82df0b5c3e70018f2d4745d66ae6da9398234ebda2ca4d02992613cb377b9651282c4f3fd0c5a3c5bc33cc3ae0"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0030	<CryptographicLength type="Integer" value="256"/>
0031	</KeyBlock>
0032	</PrivateKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="1"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>

0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
0050	value="\$UNIQUE_IDENTIFIER_0"/>
0051	</ResponsePayload>
0052	</BatchItem>
0053	</ResponseMessage>
0054	# TIME 1
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="1"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="Register"/>
0065	<RequestPayload>
0066	<ObjectType type="Enumeration" value="PublicKey"/>
0067	<TemplateAttribute>
0068	<Attribute>
0069	<AttributeName type="TextString" value="Cryptographic
0070	Usage Mask"/>
0071	<AttributeValue type="Integer" value="Verify"/>
0072	</Attribute>
0073	<Attribute>
0074	<AttributeName type="TextString" value="Link"/>
0075	<AttributeValue>
0076	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0077	<LinkedObjectIdentifier type="TextString"
0078	value="\$UNIQUE_IDENTIFIER_0"/>
0079	</AttributeValue>
0080	</Attribute>
0081	<Attribute>
0082	<AttributeName type="TextString" value="x-ID"/>
0083	<AttributeValue type="TextString" value="TC-ECC-2-11-
0084	pubkey1"/>
0085	</Attribute>
0086	</TemplateAttribute>
0087	<PublicKey>
0088	<KeyBlock>
0089	<KeyFormatType type="Enumeration" value="X_509"/>
0090	<KeyValue>
0091	<KeyMaterial type="ByteString"
0092	value="3059301306072a8648ce3d020106082a8648ce3d03010703420004b344392
0093	fb72aa267f86d7d837de1d96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aa
0094	d8dcab25b282ca8a1cf00bef7cb18a0f5ea44493a30a6d223b25b"/>
0095	</KeyValue>
0096	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
	<CryptographicLength type="Integer" value="256"/>
	</KeyBlock>
	</PublicKey>
	</RequestPayload>
	</BatchItem>
	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>

0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="1"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0109	</ResponsePayload>
0110	</BatchItem>
0111	</ResponseMessage>
# TIME 2	
0112	<RequestMessage>
0113	<RequestHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="1"/>
0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="AddAttribute"/>
0122	<RequestPayload>
0123	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Link"/>
0126	<AttributeValue>
0127	<LinkType type="Enumeration" value="PublicKeyLink"/>
0128	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0129	</AttributeValue>
0130	</Attribute>
0131	</RequestPayload>
0132	</BatchItem>
0133	</RequestMessage>
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="1"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="AddAttribute"/>
0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0148	<Attribute>

0149	<AttributeName type="TextString" value="Link"/>
0150	<AttributeValue>
0151	<LinkType type="Enumeration" value="PublicKeyLink"/>
0152	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0153	</AttributeValue>
0154	</Attribute>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
	# TIME 3
0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="1"/>
0163	</ProtocolVersion>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Locate"/>
0168	<RequestPayload>
0169	<Attribute>
0170	<AttributeName type="TextString" value="Object Type"/>
0171	<AttributeValue type="Enumeration" value="PublicKey"/>
0172	</Attribute>
0173	<Attribute>
0174	<AttributeName type="TextString" value="Link"/>
0175	<AttributeValue>
0176	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0177	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0178	</AttributeValue>
0179	</Attribute>
0180	</RequestPayload>
0181	</BatchItem>
0182	</RequestMessage>
0183	<ResponseMessage>
0184	<ResponseHeader>
0185	<ProtocolVersion>
0186	<ProtocolVersionMajor type="Integer" value="1"/>
0187	<ProtocolVersionMinor type="Integer" value="1"/>
0188	</ProtocolVersion>
0189	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0190	<BatchCount type="Integer" value="1"/>
0191	</ResponseHeader>
0192	<BatchItem>
0193	<Operation type="Enumeration" value="Locate"/>
0194	<ResultStatus type="Enumeration" value="Success"/>
0195	<ResponsePayload>
0196	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0197	</ResponsePayload>
0198	</BatchItem>
0199	</ResponseMessage>
	# TIME 4

0200	<RequestMessage>
0201	<RequestHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="1"/>
0205	</ProtocolVersion>
0206	<BatchCount type="Integer" value="1"/>
0207	</RequestHeader>
0208	<BatchItem>
0209	<Operation type="Enumeration" value="Locate"/>
0210	<RequestPayload>
0211	<Attribute>
0212	<AttributeName type="TextString" value="Object Type"/>
0213	<AttributeValue type="Enumeration" value="PrivateKey"/>
0214	</Attribute>
0215	<Attribute>
0216	<AttributeName type="TextString" value="Link"/>
0217	<AttributeValue>
0218	<LinkType type="Enumeration" value="PublicKeyLink"/>
0219	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0220	</AttributeValue>
0221	</Attribute>
0222	</RequestPayload>
0223	</BatchItem>
0224	</RequestMessage>
0225	<ResponseMessage>
0226	<ResponseHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="1"/>
0230	</ProtocolVersion>
0231	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0232	<BatchCount type="Integer" value="1"/>
0233	</ResponseHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="Locate"/>
0236	<ResultStatus type="Enumeration" value="Success"/>
0237	<ResponsePayload>
0238	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0239	</ResponsePayload>
0240	</BatchItem>
0241	</ResponseMessage>
	# TIME 5
0242	<RequestMessage>
0243	<RequestHeader>
0244	<ProtocolVersion>
0245	<ProtocolVersionMajor type="Integer" value="1"/>
0246	<ProtocolVersionMinor type="Integer" value="1"/>
0247	</ProtocolVersion>
0248	<BatchCount type="Integer" value="1"/>
0249	</RequestHeader>
0250	<BatchItem>
0251	<Operation type="Enumeration" value="Get"/>
0252	<RequestPayload>
0253	<UniqueIdentifier type="TextString"

0254	value="\$UNIQUE_IDENTIFIER_0"/>
0255	</RequestPayload>
0256	</BatchItem>
0257	</RequestMessage>
0257	<ResponseMessage>
0258	<ResponseHeader>
0259	<ProtocolVersion>
0260	<ProtocolVersionMajor type="Integer" value="1"/>
0261	<ProtocolVersionMinor type="Integer" value="1"/>
0262	</ProtocolVersion>
0263	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0264	<BatchCount type="Integer" value="1"/>
0265	</ResponseHeader>
0266	<BatchItem>
0267	<Operation type="Enumeration" value="Get"/>
0268	<ResultStatus type="Enumeration" value="Success"/>
0269	<ResponsePayload>
0270	<ObjectType type="Enumeration" value="PrivateKey"/>
0271	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0272	<PrivateKey>
0273	<KeyBlock>
0274	<KeyFormatType type="Enumeration" value="PKCS_8"/>
0275	<KeyValue>
0276	<KeyMaterial type="ByteString"
	value="3081b1301c060a2a864886f70d010c0103300e04082f2656a336573139020 20800048190eadf76e9cee21053b01c53e175b0e8c4d627c17dalb2df47d8cfb35a0 d7252a9a6488660d61235be735178d0ca8548871567c22803d8f6f6009f05c26429c 83ab72d0f2e7e7870befc3ec746f52d0eccafe34b72a791e9535b34f584b96dc1240 34e8a82df0b5c3e70018f2d4745d66ae6da9398234ebda2ca4d02992613cb377b965 1282c4f3fd0c5a3c5bc33cc3ae0"/>
0277	</KeyValue>
0278	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0279	<CryptographicLength type="Integer" value="256"/>
0280	</KeyBlock>
0281	</PrivateKey>
0282	</ResponsePayload>
0283	</BatchItem>
0284	</ResponseMessage>
	# TIME 6
0285	<RequestMessage>
0286	<RequestHeader>
0287	<ProtocolVersion>
0288	<ProtocolVersionMajor type="Integer" value="1"/>
0289	<ProtocolVersionMinor type="Integer" value="1"/>
0290	</ProtocolVersion>
0291	<BatchCount type="Integer" value="1"/>
0292	</RequestHeader>
0293	<BatchItem>
0294	<Operation type="Enumeration" value="Get"/>
0295	<RequestPayload>
0296	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0297	</RequestPayload>
0298	</BatchItem>
0299	</RequestMessage>

0300	<ResponseMessage>
0301	<ResponseHeader>
0302	<ProtocolVersion>
0303	<ProtocolVersionMajor type="Integer" value="1"/>
0304	<ProtocolVersionMinor type="Integer" value="1"/>
0305	</ProtocolVersion>
0306	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0307	<BatchCount type="Integer" value="1"/>
0308	</ResponseHeader>
0309	<BatchItem>
0310	<Operation type="Enumeration" value="Get"/>
0311	<ResultStatus type="Enumeration" value="Success"/>
0312	<ResponsePayload>
0313	<ObjectType type="Enumeration" value="PublicKey"/>
0314	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0315	<PublicKey>
0316	<KeyBlock>
0317	<KeyFormatType type="Enumeration" value="X_509"/>
0318	<KeyValue>
0319	<KeyMaterial type="ByteString"
	value="3059301306072a8648ce3d020106082a8648ce3d03010703420004b344392fb72aa267f86d7d837de1d96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aad8dcab25b282ca8a1cf00bef7cb18a0f5ea44493a30a6d223b25b"/>
0320	</KeyValue>
0321	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0322	<CryptographicLength type="Integer" value="256"/>
0323	</KeyBlock>
0324	</PublicKey>
0325	</ResponsePayload>
0326	</BatchItem>
0327	</ResponseMessage>
# TIME 7	
0328	<RequestMessage>
0329	<RequestHeader>
0330	<ProtocolVersion>
0331	<ProtocolVersionMajor type="Integer" value="1"/>
0332	<ProtocolVersionMinor type="Integer" value="1"/>
0333	</ProtocolVersion>
0334	<BatchCount type="Integer" value="1"/>
0335	</RequestHeader>
0336	<BatchItem>
0337	<Operation type="Enumeration" value="Destroy"/>
0338	<RequestPayload>
0339	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0340	</RequestPayload>
0341	</BatchItem>
0342	</RequestMessage>
0343	<ResponseMessage>
0344	<ResponseHeader>
0345	<ProtocolVersion>
0346	<ProtocolVersionMajor type="Integer" value="1"/>
0347	<ProtocolVersionMinor type="Integer" value="1"/>
0348	</ProtocolVersion>
0349	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0350	<BatchCount type="Integer" value="1"/>

0351	</ResponseHeader>
0352	<BatchItem>
0353	<Operation type="Enumeration" value="Destroy"/>
0354	<ResultStatus type="Enumeration" value="Success"/>
0355	<ResponsePayload>
0356	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0357	</ResponsePayload>
0358	</BatchItem>
0359	</ResponseMessage>
# TIME 8	
0360	<RequestMessage>
0361	<RequestHeader>
0362	<ProtocolVersion>
0363	<ProtocolVersionMajor type="Integer" value="1"/>
0364	<ProtocolVersionMinor type="Integer" value="1"/>
0365	</ProtocolVersion>
0366	<BatchCount type="Integer" value="1"/>
0367	</RequestHeader>
0368	<BatchItem>
0369	<Operation type="Enumeration" value="Destroy"/>
0370	<RequestPayload>
0371	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0372	</RequestPayload>
0373	</BatchItem>
0374	</RequestMessage>
0375	<ResponseMessage>
0376	<ResponseHeader>
0377	<ProtocolVersion>
0378	<ProtocolVersionMajor type="Integer" value="1"/>
0379	<ProtocolVersionMinor type="Integer" value="1"/>
0380	</ProtocolVersion>
0381	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0382	<BatchCount type="Integer" value="1"/>
0383	</ResponseHeader>
0384	<BatchItem>
0385	<Operation type="Enumeration" value="Destroy"/>
0386	<ResultStatus type="Enumeration" value="Success"/>
0387	<ResponsePayload>
0388	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0389	</ResponsePayload>
0390	</BatchItem>
0391	</ResponseMessage>

691

692 2.2.41 TC-ECC-3-11 - Register an ECC Key Pair and ECDSA Certificate

693 EC recommended curve is P-256 (secp256r1)

694 - Private Key format ECPrivateKey - <http://tools.ietf.org/html/rfc5915>

695 - Public Key format SubjectPublicKeyInfo - <http://tools.ietf.org/html/rfc5480>

696 Register a EC private key in the ECPrivateKey key format, then register the corresponding public
697 key, in X.509 (SubjectPublicKeyInfo) format, and a corresponding ECDSA certificate, with the
698 Link attribute pointing to the previously registered private key. Return the attribute values for
699 the ECDSA certificate showing the correct server parsing of the certificate. Then add the Link
700 attribute to the private key, and perform Locate operations to find the public and private keys
701 using the Link attribute. Get both the private and public keys in default format, then destroy
702 both the private and the public key.

703

```

704 -----BEGIN EC PRIVATE KEY-----
705 MHcCAQEEIJEqDiCPXdc0sYUYR+RlnEWISW2f08GtpRDqLJadr570oAoGCCqGSM49
706 AwEHoUQDQgAEs0Q5L7cqomf4bX2DfeHZbOlg/8Bc7vPx+ibYVGpkQvPBOX6Smq2N
707 yrJbKCyooc8AvvFLGKD16kRJOjCm0iOyWw==
708 -----END EC PRIVATE KEY-----
709
710 -----BEGIN PUBLIC KEY-----
711 MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEs0Q5L7cqomf4bX2DfeHZbOlg/8Bc
712 7vPx+ibYVGpkQvPBOX6Smq2NyrJbKCyooc8AvvFLGKD16kRJOjCm0iOyWw==
713 -----END PUBLIC KEY-----
714
715 -----BEGIN CERTIFICATE-----
716 MIIB1zCCAX2gAwIBAgIJANraFqWKNSTZMAoGCCqGSM49BAMCMExCzAJBgNVBAYT
717 AlVTMQ0wCwYDVQQKDARURVNUMQ4wDAYDVQQQLDAVPQVNJUzEaMBGGA1UEAwRS01J
718 UC1FQy1zZWNVmJyU2cjEwHhcNMjMwNjI0MDM1NDQzWhcNMjMwNjI0MDM1NDQzWjBI
719 MQswCQYDVQQGEwJVUzENMAAsGA1UECgwEVEVTVDEOMAwGA1UECwwFT0FTSVMxGjAY
720 BgNVBAMMEUtNSVAtRUMtc2VjcDI1NnIxMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcD
721 QgAEs0Q5L7cqomf4bX2DfeHZbOlg/8Bc7vPx+ibYVGpkQvPBOX6Smq2NyrJbKCyo
722 oc8AvvFLGKD16kRJOjCm0iOyW6NQME4wHQYDVR0OBBYEFMDL251FazsUho/ZyIZ9
723 4Pzf79STMB8GA1UdIwQYMBaAFMDL251FazsUho/ZyIZ94Pzf79STMAwGA1UdEwQF
724 MAMBAf8wCgYIKoZIzj0EAwIDSAAwRQIgI19fyzddlgavOhIaeHbOnBoV0ldEmg6q
725 YA+OemaQS98CIQCpuF4UPYklouwi8hDTVavL3MAX/9Cm82CRf1fshp7RQ==
726 -----END CERTIFICATE-----
727
728
```

#	TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="PrivateKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Sign"/>
0017	</Attribute>

0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-ECC-3-11-
	prikey1"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<PrivateKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="ECPrivateKey"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString"
	value="30770201010420912a0e208f5dd734b1851847e4659c4588b16d9f3bc1ada
	510ea2c969daf9ef4a00a06082a8648ce3d030107a14403420004b344392fb72aa26
	7f86d7d837de1d96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aad8dcab25
	b282ca8alcf00bef7cb18a0f5ea44493a30a6d223b25b"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0030	<CryptographicLength type="Integer" value="256"/>
0031	</KeyBlock>
0032	</PrivateKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="1"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="1"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PublicKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic

0068	Usage Mask"/>
0069	<AttributeValue type="Integer" value="Verify"/>
0070	</Attribute>
0071	<Attribute>
0072	<AttributeName type="TextString" value="Link"/>
0073	<AttributeValue>
0074	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0075	<LinkedObjectIdentifier type="TextString"
0076	value="\$UNIQUE_IDENTIFIER_0"/>
0077	</Attribute>
0078	</Attribute>
0079	<AttributeName type="TextString" value="x-ID"/>
0080	<AttributeValue type="TextString" value="TC-ECC-3-11-
0081	pubkey1"/>
0082	</Attribute>
0083	</TemplateAttribute>
0084	<PublicKey>
0085	<KeyBlock>
0086	<KeyFormatType type="Enumeration" value="X_509"/>
0087	<KeyValue>
0088	<KeyMaterial type="ByteString"
0089	value="3059301306072a8648ce3d020106082a8648ce3d03010703420004b344392
0090	fb72aa267f86d7d837de1d96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aa
0091	d8dcab25b282ca8a1cf00bef7cb18a0f5ea44493a30a6d223b25b"/>
0092	</KeyValue>
0093	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0094	<CryptographicLength type="Integer" value="256"/>
0095	</KeyBlock>
0096	</PublicKey>
0097	</RequestPayload>
0098	</BatchItem>
0099	</RequestMessage>
0100	</ResponseMessage>
0101	<ResponseMessage>
0102	<ResponseHeader>
0103	<ProtocolVersion>
0104	<ProtocolVersionMajor type="Integer" value="1"/>
0105	<ProtocolVersionMinor type="Integer" value="1"/>
0106	</ProtocolVersion>
0107	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0108	<BatchCount type="Integer" value="1"/>
0109	</ResponseHeader>
0110	<BatchItem>
0111	<Operation type="Enumeration" value="Register"/>
0112	<ResultStatus type="Enumeration" value="Success"/>
0113	<ResponsePayload>
0114	<UniqueIdentifier type="TextString"
0115	value="\$UNIQUE_IDENTIFIER_1"/>
0116	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>
	# TIME 2
	<RequestMessage>
	<RequestHeader>
	<ProtocolVersion>
	<ProtocolVersionMajor type="Integer" value="1"/>
	<ProtocolVersionMinor type="Integer" value="1"/>

0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="Register"/>
0122	<RequestPayload>
0123	<ObjectType type="Enumeration" value="Certificate"/>
0124	<TemplateAttribute>
0125	<Attribute>
0126	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0127	<AttributeValue type="Integer" value="Verify Sign"/>
0128	</Attribute>
0129	<Attribute>
0130	<AttributeName type="TextString" value="Link"/>
0131	<AttributeValue>
0132	<LinkType type="Enumeration" value="PublicKeyLink"/>
0133	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0134	</AttributeValue>
0135	</Attribute>
0136	<Attribute>
0137	<AttributeName type="TextString" value="x-ID"/>
0138	<AttributeValue type="TextString" value="TC-ECC-3-11- cert1"/>
0139	</Attribute>
0140	</TemplateAttribute>
0141	<Certificate>
0142	<CertificateType type="Enumeration" value="X_509"/>
0143	<CertificateValue type="ByteString" value="308201d73082017da003020102020900dada16a58d2924d9300a06082a864 8ce3d0403023048310b3009060355040613025553310d300b060355040a0c0454455 354310e300c060355040b0c054f41534953311a301806035504030c114b4d49502d4 5432d736563703235367231301e170d3133303632363033353434335a170d3233303 632343033353434335a3048310b3009060355040613025553310d300b060355040a0 c0454455354310e300c060355040b0c054f41534953311a301806035504030c114b4 d49502d45432d7365637032353672313059301306072a8648ce3d020106082a8648c e3d03010703420004b344392fb72aa267f86d7d837de1d96ce960ffc05ceef3f1fa2 6d8546a6442f3c1397e929aad8dcab25b282ca8a1cf00bef7cb18a0f5ea44493a30a 6d223b25ba350304e301d0603551d0e04160414c74bdb9d456b3b14868fd9c8867de 0fcdfeffd493301f0603551d23041830168014c74bdb9d456b3b14868fd9c8867de0f cdfefd493300c0603551d13040530030101ff300a06082a8648ce3d0403020348003 0450220235f5fcb375dd606af3a121a7876ce9c1a15d257449a0eaa600f8e1266904 bdf022100a9b85e143d8925a2ebb08bc8434d56af2f73005fff429bcd8245fd5fb21 a7b45"/>
0144	</Certificate>
0145	</RequestPayload>
0146	</BatchItem>
0147	</RequestMessage>
0148	<ResponseMessage>
0149	<ResponseHeader>
0150	<ProtocolVersion>
0151	<ProtocolVersionMajor type="Integer" value="1"/>
0152	<ProtocolVersionMinor type="Integer" value="1"/>
0153	</ProtocolVersion>
0154	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0155	<BatchCount type="Integer" value="1"/>

0156	</ResponseHeader>
0157	<BatchItem>
0158	<Operation type="Enumeration" value="Register"/>
0159	<ResultStatus type="Enumeration" value="Success"/>
0160	<ResponsePayload>
0161	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0162	</ResponsePayload>
0163	</BatchItem>
0164	</ResponseMessage>
# TIME 3	
0165	<RequestMessage>
0166	<RequestHeader>
0167	<ProtocolVersion>
0168	<ProtocolVersionMajor type="Integer" value="1"/>
0169	<ProtocolVersionMinor type="Integer" value="1"/>
0170	</ProtocolVersion>
0171	<BatchCount type="Integer" value="2"/>
0172	</RequestHeader>
0173	<BatchItem>
0174	<Operation type="Enumeration" value="AddAttribute"/>
0175	<UniqueBatchItemID type="ByteString" value="01"/>
0176	<RequestPayload>
0177	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0178	<Attribute>
0179	<AttributeName type="TextString" value="Link"/>
0180	<AttributeValue>
0181	<LinkType type="Enumeration" value="PublicKeyLink"/>
0182	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0183	</AttributeValue>
0184	</Attribute>
0185	</RequestPayload>
0186	</BatchItem>
0187	<BatchItem>
0188	<Operation type="Enumeration" value="AddAttribute"/>
0189	<UniqueBatchItemID type="ByteString" value="02"/>
0190	<RequestPayload>
0191	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0192	<Attribute>
0193	<AttributeName type="TextString" value="Link"/>
0194	<AttributeValue>
0195	<LinkType type="Enumeration" value="CertificateLink"/>
0196	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0197	</AttributeValue>
0198	</Attribute>
0199	</RequestPayload>
0200	</BatchItem>
0201	</RequestMessage>
0202	<ResponseMessage>
0203	<ResponseHeader>
0204	<ProtocolVersion>
0205	<ProtocolVersionMajor type="Integer" value="1"/>
0206	<ProtocolVersionMinor type="Integer" value="1"/>

0207	</ProtocolVersion>
0208	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0209	<BatchCount type="Integer" value="2"/>
0210	</ResponseHeader>
0211	<BatchItem>
0212	<Operation type="Enumeration" value="AddAttribute"/>
0213	<UniqueBatchItemID type="ByteString" value="01"/>
0214	<ResultStatus type="Enumeration" value="Success"/>
0215	<ResponsePayload>
0216	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0217	<Attribute>
0218	<AttributeName type="TextString" value="Link"/>
0219	<AttributeValue>
0220	<LinkType type="Enumeration" value="PublicKeyLink"/>
0221	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0222	</AttributeValue>
0223	</Attribute>
0224	</ResponsePayload>
0225	</BatchItem>
0226	<BatchItem>
0227	<Operation type="Enumeration" value="AddAttribute"/>
0228	<UniqueBatchItemID type="ByteString" value="02"/>
0229	<ResultStatus type="Enumeration" value="Success"/>
0230	<ResponsePayload>
0231	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0232	<Attribute>
0233	<AttributeName type="TextString" value="Link"/>
0234	<AttributeIndex type="Integer" value="1"/>
0235	<AttributeValue>
0236	<LinkType type="Enumeration" value="CertificateLink"/>
0237	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0238	</AttributeValue>
0239	</Attribute>
0240	</ResponsePayload>
0241	</BatchItem>
0242	</ResponseMessage>
# TIME 4	
0243	<RequestMessage>
0244	<RequestHeader>
0245	<ProtocolVersion>
0246	<ProtocolVersionMajor type="Integer" value="1"/>
0247	<ProtocolVersionMinor type="Integer" value="1"/>
0248	</ProtocolVersion>
0249	<BatchCount type="Integer" value="1"/>
0250	</RequestHeader>
0251	<BatchItem>
0252	<Operation type="Enumeration" value="GetAttributeList"/>
0253	<RequestPayload>
0254	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0255	</RequestPayload>
0256	</BatchItem>
0257	</RequestMessage>

0258	<ResponseMessage>
0259	<ResponseHeader>
0260	<ProtocolVersion>
0261	<ProtocolVersionMajor type="Integer" value="1"/>
0262	<ProtocolVersionMinor type="Integer" value="1"/>
0263	</ProtocolVersion>
0264	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0265	<BatchCount type="Integer" value="1"/>
0266	</ResponseHeader>
0267	<BatchItem>
0268	<Operation type="Enumeration" value="GetAttributeList"/>
0269	<ResultStatus type="Enumeration" value="Success"/>
0270	<ResponsePayload>
0271	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0272	<AttributeName type="TextString" value="x-ID"/>
0273	<AttributeName type="TextString" value="Unique Identifier"/>
0274	<AttributeName type="TextString" value="Object Type"/>
0275	<AttributeName type="TextString" value="Certificate Type"/>
0276	<AttributeName type="TextString" value="Certificate
	Identifier"/>
0277	<AttributeName type="TextString" value="Certificate Issuer"/>
0278	<AttributeName type="TextString" value="Certificate Length"/>
0279	<AttributeName type="TextString" value="Certificate Subject"/>
0280	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0281	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0282	<AttributeName type="TextString" value="Digest"/>
0283	<AttributeName type="TextString" value="Digital Signature
	Algorithm"/>
0284	<AttributeName type="TextString" value="Fresh"/>
0285	<AttributeName type="TextString" value="Initial Date"/>
0286	<AttributeName type="TextString" value="Last Change Date"/>
0287	<AttributeName type="TextString" value="Lease Time"/>
0288	<AttributeName type="TextString" value="Link"/>
0289	<AttributeName type="TextString" value="State"/>
0290	<AttributeName type="TextString" value="X.509 Certificate
	Identifier"/>
0291	<AttributeName type="TextString" value="X.509 Certificate
	Issuer"/>
0292	<AttributeName type="TextString" value="X.509 Certificate
	Subject"/>
0293	</ResponsePayload>
0294	</BatchItem>
0295	</ResponseMessage>
	# TIME 5
0296	<RequestMessage>
0297	<RequestHeader>
0298	<ProtocolVersion>
0299	<ProtocolVersionMajor type="Integer" value="1"/>
0300	<ProtocolVersionMinor type="Integer" value="1"/>
0301	</ProtocolVersion>
0302	<BatchCount type="Integer" value="1"/>
0303	</RequestHeader>
0304	<BatchItem>
0305	<Operation type="Enumeration" value="GetAttributes"/>

0306	<RequestPayload>
0307	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0308	<AttributeName type="TextString" value="Digital Signature
	Algorithm"/>
0309	<AttributeName type="TextString" value="X.509 Certificate
	Identifier"/>
0310	<AttributeName type="TextString" value="X.509 Certificate
	Issuer"/>
0311	<AttributeName type="TextString" value="X.509 Certificate
	Subject"/>
0312	</RequestPayload>
0313	</BatchItem>
0314	</RequestMessage>
0315	<ResponseMessage>
0316	<ResponseHeader>
0317	<ProtocolVersion>
0318	<ProtocolVersionMajor type="Integer" value="1"/>
0319	<ProtocolVersionMinor type="Integer" value="1"/>
0320	</ProtocolVersion>
0321	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0322	<BatchCount type="Integer" value="1"/>
0323	</ResponseHeader>
0324	<BatchItem>
0325	<Operation type="Enumeration" value="GetAttributes"/>
0326	<ResultStatus type="Enumeration" value="Success"/>
0327	<ResponsePayload>
0328	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0329	<Attribute>
0330	<AttributeName type="TextString" value="Digital Signature
	Algorithm"/>
0331	<AttributeValue type="Enumeration" value="ECDSAWithSHA256"/>
0332	</Attribute>
0333	<Attribute>
0334	<AttributeName type="TextString" value="X.509 Certificate
	Identifier"/>
0335	<AttributeValue>
0336	<IssuerDistinguishedName type="ByteString"
	value="3048310b3009060355040613025553310d300b060355040a0c04544553543
	10e300c060355040b0c054f41534953311a301806035504030c114b4d49502d45432
	d736563703235366b31"/>
0337	<CertificateSerialNumber type="ByteString"
	value="020900ec0b7402196d5295"/>
0338	</AttributeValue>
0339	</Attribute>
0340	<Attribute>
0341	<AttributeName type="TextString" value="X.509 Certificate
	Issuer"/>
0342	<AttributeValue>
0343	<IssuerDistinguishedName type="ByteString"
	value="3048310b3009060355040613025553310d300b060355040a0c04544553543
	10e300c060355040b0c054f41534953311a301806035504030c114b4d49502d45432
	d736563703235366b31"/>
0344	</AttributeValue>
0345	</Attribute>
0346	</Attribute>

0347	<AttributeName type="TextString" value="X.509 Certificate Subject"/>
0348	<AttributeValue>
0349	<SubjectDistinguishedName type="ByteString" value="3048310b3009060355040613025553310d300b060355040a0c0454455354310e300c060355040b0c054f41534953311a301806035504030c114b4d49502d45432d736563703235366b31"/>
0350	</AttributeValue>
0351	</Attribute>
0352	</ResponsePayload>
0353	</BatchItem>
0354	</ResponseMessage>
# TIME 6	
0355	<RequestMessage>
0356	<RequestHeader>
0357	<ProtocolVersion>
0358	<ProtocolVersionMajor type="Integer" value="1"/>
0359	<ProtocolVersionMinor type="Integer" value="1"/>
0360	</ProtocolVersion>
0361	<BatchCount type="Integer" value="1"/>
0362	</RequestHeader>
0363	<BatchItem>
0364	<Operation type="Enumeration" value="Locate"/>
0365	<RequestPayload>
0366	<Attribute>
0367	<AttributeName type="TextString" value="Object Type"/>
0368	<AttributeValue type="Enumeration" value="PublicKey"/>
0369	</Attribute>
0370	<Attribute>
0371	<AttributeName type="TextString" value="Link"/>
0372	<AttributeValue>
0373	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0374	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0375	</AttributeValue>
0376	</Attribute>
0377	</RequestPayload>
0378	</BatchItem>
0379	</RequestMessage>
0380	<ResponseMessage>
0381	<ResponseHeader>
0382	<ProtocolVersion>
0383	<ProtocolVersionMajor type="Integer" value="1"/>
0384	<ProtocolVersionMinor type="Integer" value="1"/>
0385	</ProtocolVersion>
0386	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0387	<BatchCount type="Integer" value="1"/>
0388	</ResponseHeader>
0389	<BatchItem>
0390	<Operation type="Enumeration" value="Locate"/>
0391	<ResultStatus type="Enumeration" value="Success"/>
0392	<ResponsePayload>
0393	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0394	</ResponsePayload>
0395	</BatchItem>
0396	</ResponseMessage>

0397 0398 0399 0400 0401 0402 0403 0404 0405 0406 0407 0408 0409 0410 0411 0412 0413 0414 0415 0416 0417 0418 0419 0420 0421	<pre> # TIME 7 <RequestMessage> <RequestHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="1"/> </ProtocolVersion> <BatchCount type="Integer" value="1"/> </RequestHeader> <BatchItem> <Operation type="Enumeration" value="Locate"/> <RequestPayload> <Attribute> <AttributeName type="TextString" value="Object Type"/> <AttributeValue type="Enumeration" value="PrivateKey"/> </Attribute> <Attribute> <AttributeName type="TextString" value="Link"/> <AttributeValue> <LinkType type="Enumeration" value="PublicKeyLink"/> <LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> </AttributeValue> </Attribute> </RequestPayload> </BatchItem> </RequestMessage> </pre>
0422 0423 0424 0425 0426 0427 0428 0429 0430 0431 0432 0433 0434 0435 0436 0437 0438	<pre> <ResponseMessage> <ResponseHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="1"/> </ProtocolVersion> <TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/> <BatchCount type="Integer" value="1"/> </ResponseHeader> <BatchItem> <Operation type="Enumeration" value="Locate"/> <ResultStatus type="Enumeration" value="Success"/> <ResponsePayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/> </ResponsePayload> </BatchItem> </ResponseMessage> </pre>
0439 0440 0441 0442 0443 0444 0445 0446 0447 0448 0449	<pre> # TIME 8 <RequestMessage> <RequestHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="1"/> </ProtocolVersion> <BatchCount type="Integer" value="1"/> </RequestHeader> <BatchItem> <Operation type="Enumeration" value="Get"/> <RequestPayload> </pre>

0450	<UniqueIdentifier type="TextString"
0451	value="\$UNIQUE_IDENTIFIER_0"/>
0452	</RequestPayload>
0453	</BatchItem>
0454	</RequestMessage>
0454	<ResponseMessage>
0455	<ResponseHeader>
0456	<ProtocolVersion>
0457	<ProtocolVersionMajor type="Integer" value="1"/>
0458	<ProtocolVersionMinor type="Integer" value="1"/>
0459	</ProtocolVersion>
0460	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0461	<BatchCount type="Integer" value="1"/>
0462	</ResponseHeader>
0463	<BatchItem>
0464	<Operation type="Enumeration" value="Get"/>
0465	<ResultStatus type="Enumeration" value="Success"/>
0466	<ResponsePayload>
0467	<ObjectType type="Enumeration" value="PrivateKey"/>
0468	<UniqueIdentifier type="TextString"
0469	value="\$UNIQUE_IDENTIFIER_0"/>
0470	<PrivateKey>
0471	<KeyBlock>
0472	<KeyFormatType type="Enumeration" value="ECPrivateKey"/>
0473	<KeyValue>
0474	<KeyMaterial type="ByteString"
0475	value="3081b1301c060a2a864886f70d010c0103300e04082f2656a336573139020
0476	20800048190eadf76e9cee21053b01c53e175b0e8c4d627c17da1b2df47d8cfb35a0
0477	d7252a9a6488660d61235be735178d0ca8548871567c22803d8f6f6009f05c26429c
0478	83ab72d0f2e7e7870befc3ec746f52d0eccafe34b72a791e9535b34f584b96dc1240
0479	34e8a82df0b5c3e70018f2d4745d66ae6da9398234ebda2ca4d02992613cb377b965
0480	1282c4f3fd0c5a3c5bc33cc3ae0"/>
0481	</KeyValue>
0482	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0483	<CryptographicLength type="Integer" value="256"/>
0484	</KeyBlock>
0485	</PrivateKey>
0486	</ResponsePayload>
0487	</BatchItem>
0488	</ResponseMessage>
0482	# TIME 9
0482	<RequestMessage>
0483	<RequestHeader>
0484	<ProtocolVersion>
0485	<ProtocolVersionMajor type="Integer" value="1"/>
0486	<ProtocolVersionMinor type="Integer" value="1"/>
0487	</ProtocolVersion>
0488	<BatchCount type="Integer" value="1"/>
0489	</RequestHeader>
0490	<BatchItem>
0491	<Operation type="Enumeration" value="Get"/>
0492	<RequestPayload>
0493	<UniqueIdentifier type="TextString"
0494	value="\$UNIQUE_IDENTIFIER_1"/>
0495	</RequestPayload>
0496	</BatchItem>
0496	</RequestMessage>

0497	<ResponseMessage>
0498	<ResponseHeader>
0499	<ProtocolVersion>
0500	<ProtocolVersionMajor type="Integer" value="1"/>
0501	<ProtocolVersionMinor type="Integer" value="1"/>
0502	</ProtocolVersion>
0503	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0504	<BatchCount type="Integer" value="1"/>
0505	</ResponseHeader>
0506	<BatchItem>
0507	<Operation type="Enumeration" value="Get"/>
0508	<ResultStatus type="Enumeration" value="Success"/>
0509	<ResponsePayload>
0510	<ObjectType type="Enumeration" value="PublicKey"/>
0511	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0512	<PublicKey>
0513	<KeyBlock>
0514	<KeyFormatType type="Enumeration" value="X_509"/>
0515	<KeyValue>
0516	<KeyMaterial type="ByteString"
	value="3059301306072a8648ce3d020106082a8648ce3d03010703420004b344392
	fb72aa267f86d7d837de1d96ce960ffc05ceef3f1fa26d8546a6442f3c1397e929aa
	d8dcab25b282ca8a1cf00bef7cb18a0f5ea44493a30a6d223b25b"/>
0517	</KeyValue>
0518	<CryptographicAlgorithm type="Enumeration" value="ECDSA"/>
0519	<CryptographicLength type="Integer" value="256"/>
0520	</KeyBlock>
0521	</PublicKey>
0522	</ResponsePayload>
0523	</BatchItem>
0524	</ResponseMessage>
	# TIME 10
0525	<RequestMessage>
0526	<RequestHeader>
0527	<ProtocolVersion>
0528	<ProtocolVersionMajor type="Integer" value="1"/>
0529	<ProtocolVersionMinor type="Integer" value="1"/>
0530	</ProtocolVersion>
0531	<BatchCount type="Integer" value="1"/>
0532	</RequestHeader>
0533	<BatchItem>
0534	<Operation type="Enumeration" value="Destroy"/>
0535	<RequestPayload>
0536	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0537	</RequestPayload>
0538	</BatchItem>
0539	</RequestMessage>
0540	<ResponseMessage>
0541	<ResponseHeader>
0542	<ProtocolVersion>
0543	<ProtocolVersionMajor type="Integer" value="1"/>
0544	<ProtocolVersionMinor type="Integer" value="1"/>
0545	</ProtocolVersion>
0546	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0547	<BatchCount type="Integer" value="1"/>

0548	</ResponseHeader>
0549	<BatchItem>
0550	<Operation type="Enumeration" value="Destroy"/>
0551	<ResultStatus type="Enumeration" value="Success"/>
0552	<ResponsePayload>
0553	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0554	</ResponsePayload>
0555	</BatchItem>
0556	</ResponseMessage>
# TIME 11	
0557	<RequestMessage>
0558	<RequestHeader>
0559	<ProtocolVersion>
0560	<ProtocolVersionMajor type="Integer" value="1"/>
0561	<ProtocolVersionMinor type="Integer" value="1"/>
0562	</ProtocolVersion>
0563	<BatchCount type="Integer" value="1"/>
0564	</RequestHeader>
0565	<BatchItem>
0566	<Operation type="Enumeration" value="Destroy"/>
0567	<RequestPayload>
0568	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0569	</RequestPayload>
0570	</BatchItem>
0571	</RequestMessage>
0572	<ResponseMessage>
0573	<ResponseHeader>
0574	<ProtocolVersion>
0575	<ProtocolVersionMajor type="Integer" value="1"/>
0576	<ProtocolVersionMinor type="Integer" value="1"/>
0577	</ProtocolVersion>
0578	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0579	<BatchCount type="Integer" value="1"/>
0580	</ResponseHeader>
0581	<BatchItem>
0582	<Operation type="Enumeration" value="Destroy"/>
0583	<ResultStatus type="Enumeration" value="Success"/>
0584	<ResponsePayload>
0585	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0586	</ResponsePayload>
0587	</BatchItem>
0588	</ResponseMessage>
# TIME 12	
0589	<RequestMessage>
0590	<RequestHeader>
0591	<ProtocolVersion>
0592	<ProtocolVersionMajor type="Integer" value="1"/>
0593	<ProtocolVersionMinor type="Integer" value="1"/>
0594	</ProtocolVersion>
0595	<BatchCount type="Integer" value="1"/>
0596	</RequestHeader>
0597	<BatchItem>
0598	<Operation type="Enumeration" value="Destroy"/>

0599	<RequestPayload>
0600	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0601	</RequestPayload>
0602	</BatchItem>
0603	</RequestMessage>
0604	<ResponseMessage>
0605	<ResponseHeader>
0606	<ProtocolVersion>
0607	<ProtocolVersionMajor type="Integer" value="1"/>
0608	<ProtocolVersionMinor type="Integer" value="1"/>
0609	</ProtocolVersion>
0610	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0611	<BatchCount type="Integer" value="1"/>
0612	</ResponseHeader>
0613	<BatchItem>
0614	<Operation type="Enumeration" value="Destroy"/>
0615	<ResultStatus type="Enumeration" value="Success"/>
0616	<ResponsePayload>
0617	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0618	</ResponsePayload>
0619	</BatchItem>
0620	</ResponseMessage>

729

730

731

732

733 2.3 KMIP 1.2 Test Cases

734 2.3.1 TC-311-12 - Create / Destroy

735 In this test case the client issues a Create request, whereby the server creates a new symmetric
736 key and returns the Unique Identifier. To clean up, the client then performs a Destroy operation
737 to destroy the key.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>

0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
0020	Length"/>
0021	<AttributeValue type="Integer" value="128"/>
0022	</Attribute>
0023	<AttributeName type="TextString" value="Cryptographic
0024	Usage Mask"/>
0025	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0026	</Attribute>
0027	<AttributeName type="TextString" value="x-ID"/>
0028	<AttributeValue type="TextString" value="TC-311-12"/>
0029	</Attribute>
0030	</TemplateAttribute>
0031	</RequestPayload>
0032	</BatchItem>
0033	</RequestMessage>
0034	<ResponseMessage>
0035	<ResponseHeader>
0036	<ProtocolVersion>
0037	<ProtocolVersionMajor type="Integer" value="1"/>
0038	<ProtocolVersionMinor type="Integer" value="2"/>
0039	</ProtocolVersion>
0040	<TimeStamp type="DateTime" value="2012-04-27T08:12:21+00:00"/>
0041	<BatchCount type="Integer" value="1"/>
0042	</ResponseHeader>
0043	<BatchItem>
0044	<Operation type="Enumeration" value="Create"/>
0045	<ResultStatus type="Enumeration" value="Success"/>
0046	<ResponsePayload>
0047	<ObjectType type="Enumeration" value="SymmetricKey"/>
0048	<UniqueIdentifier type="TextString"
0049	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
0053	# TIME 1
0054	<RequestMessage>
0055	<RequestHeader>
0056	<ProtocolVersion>
0057	<ProtocolVersionMajor type="Integer" value="1"/>
0058	<ProtocolVersionMinor type="Integer" value="2"/>
0059	</ProtocolVersion>
0060	<BatchCount type="Integer" value="1"/>
0061	</RequestHeader>
0062	<BatchItem>
0063	<Operation type="Enumeration" value="Destroy"/>
0064	<RequestPayload>
0065	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
	</RequestPayload>
	</BatchItem>

0066	</RequestMessage>
0067	<ResponseMessage>
0068	<ResponseHeader>
0069	<ProtocolVersion>
0070	<ProtocolVersionMajor type="Integer" value="1"/>
0071	<ProtocolVersionMinor type="Integer" value="2"/>
0072	</ProtocolVersion>
0073	<TimeStamp type="DateTime" value="2012-04-27T08:12:21+00:00"/>
0074	<BatchCount type="Integer" value="1"/>
0075	</ResponseHeader>
0076	<BatchItem>
0077	<Operation type="Enumeration" value="Destroy"/>
0078	<ResultStatus type="Enumeration" value="Success"/>
0079	<ResponsePayload>
0080	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0081	</ResponsePayload>
0082	</BatchItem>
0083	</ResponseMessage>

738

739 2.3.2 TC-312-12 - Register / Create / Get attributes / Destroy

740 Here the client first registers a template object and then creates a symmetric key using the
741 registered template. To verify that the attributes of the key were set correctly from the
742 template, the client then issues a Get Attributes command, after which it destroys first the key
743 and then the template.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="Template"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Name"/>
0016	<AttributeValue>
0017	<NameValue type="TextString" value="TC-312-12-
	templatel"/>
0018	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0019	</AttributeValue>
0020	</Attribute>
0021	<Attribute>
0022	<AttributeName type="TextString" value="x-ID"/>
0023	<AttributeValue type="TextString" value="TC-312-12"/>
0024	</Attribute>

0025	</TemplateAttribute>
0026	<Template>
0027	<Attribute>
0028	<AttributeName type="TextString" value="Object Group"/>
0029	<AttributeValue type="TextString" value="Group1"/>
0030	</Attribute>
0031	<Attribute>
0032	<AttributeName type="TextString" value="Application Specific Information"/>
0033	<AttributeValue>
0034	<ApplicationNamespace type="TextString" value="ssl"/>
0035	<ApplicationData type="TextString" value="www.example.com"/>
0036	</AttributeValue>
0037	</Attribute>
0038	<Attribute>
0039	<AttributeName type="TextString" value="Contact Information"/>
0040	<AttributeValue type="TextString" value="Joe"/>
0041	</Attribute>
0042	<Attribute>
0043	<AttributeName type="TextString" value="x-Purpose"/>
0044	<AttributeValue type="TextString" value="demonstration"/>
0045	</Attribute>
0046	<Attribute>
0047	<AttributeName type="TextString" value="x-ID"/>
0048	<AttributeValue type="TextString" value="TC-312-12-from- template"/>
0049	</Attribute>
0050	</Template>
0051	</RequestPayload>
0052	</BatchItem>
0053	</RequestMessage>
0054	<ResponseMessage>
0055	<ResponseHeader>
0056	<ProtocolVersion>
0057	<ProtocolVersionMajor type="Integer" value="1"/>
0058	<ProtocolVersionMinor type="Integer" value="2"/>
0059	</ProtocolVersion>
0060	<TimeStamp type="DateTime" value="2012-04-27T08:12:21+00:00"/>
0061	<BatchCount type="Integer" value="1"/>
0062	</ResponseHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="Register"/>
0065	<ResultStatus type="Enumeration" value="Success"/>
0066	<ResponsePayload>
0067	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0068	</ResponsePayload>
0069	</BatchItem>
0070	</ResponseMessage>
	# TIME 1
0071	<RequestMessage>
0072	<RequestHeader>
0073	<ProtocolVersion>
0074	<ProtocolVersionMajor type="Integer" value="1"/>
0075	<ProtocolVersionMinor type="Integer" value="2"/>

0076	</ProtocolVersion>
0077	<BatchCount type="Integer" value="1"/>
0078	</RequestHeader>
0079	<BatchItem>
0080	<Operation type="Enumeration" value="Create"/>
0081	<RequestPayload>
0082	<ObjectType type="Enumeration" value="SymmetricKey"/>
0083	<TemplateAttribute>
0084	<Name>
0085	<NameValue type="TextString" value="TC-312-12-templatel"/>
0086	<NameType type="Enumeration"
0087	value="UninterpretedTextString"/>
0088	</Name>
0089	<Attribute>
0090	<AttributeName type="TextString" value="Cryptographic
0091	Algorithm"/>
0092	<AttributeValue type="Enumeration" value="AES"/>
0093	</Attribute>
0094	<Attribute>
0095	<AttributeName type="TextString" value="Cryptographic
0096	Length"/>
0097	<AttributeValue type="Integer" value="128"/>
0098	</Attribute>
0099	<Attribute>
0100	<AttributeName type="TextString" value="Cryptographic
0101	Usage Mask"/>
0102	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0103	</Attribute>
0104	<Attribute>
0105	<AttributeName type="TextString" value="Name"/>
0106	<AttributeValue>
0107	<NameValue type="TextString" value="TC-312-12-key1"/>
0108	<NameType type="Enumeration"
0109	value="UninterpretedTextString"/>
0110	</AttributeValue>
0111	</Attribute>
0112	<Attribute>
0113	<AttributeName type="TextString" value="x-ID"/>
0114	<AttributeValue type="TextString" value="TC-312-12-from-
0115	create"/>
0116	</Attribute>
0117	</TemplateAttribute>
0118	</RequestPayload>
0119	</BatchItem>
0120	</RequestMessage>
0121	<ResponseMessage>
0122	<ResponseHeader>
0123	<ProtocolVersion>
0124	<ProtocolVersionMajor type="Integer" value="1"/>
0125	<ProtocolVersionMinor type="Integer" value="2"/>
0126	</ProtocolVersion>
	<TimeStamp type="DateTime" value="2012-04-27T08:12:22+00:00"/>
	<BatchCount type="Integer" value="1"/>
	</ResponseHeader>
	<BatchItem>
	<Operation type="Enumeration" value="Create"/>
	<ResultStatus type="Enumeration" value="Success"/>

0127	<ResponsePayload>
0128	<ObjectType type="Enumeration" value="SymmetricKey"/>
0129	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0130	</ResponsePayload>
0131	</BatchItem>
0132	</ResponseMessage>
	# TIME 2
0133	<RequestMessage>
0134	<RequestHeader>
0135	<ProtocolVersion>
0136	<ProtocolVersionMajor type="Integer" value="1"/>
0137	<ProtocolVersionMinor type="Integer" value="2"/>
0138	</ProtocolVersion>
0139	<BatchCount type="Integer" value="1"/>
0140	</RequestHeader>
0141	<BatchItem>
0142	<Operation type="Enumeration" value="GetAttributes"/>
0143	<RequestPayload>
0144	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0145	</RequestPayload>
0146	</BatchItem>
0147	</RequestMessage>
0148	<ResponseMessage>
0149	<ResponseHeader>
0150	<ProtocolVersion>
0151	<ProtocolVersionMajor type="Integer" value="1"/>
0152	<ProtocolVersionMinor type="Integer" value="2"/>
0153	</ProtocolVersion>
0154	<TimeStamp type="DateTime" value="2012-04-27T08:12:22+00:00"/>
0155	<BatchCount type="Integer" value="1"/>
0156	</ResponseHeader>
0157	<BatchItem>
0158	<Operation type="Enumeration" value="GetAttributes"/>
0159	<ResultStatus type="Enumeration" value="Success"/>
0160	<ResponsePayload>
0161	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0162	<Attribute>
0163	<AttributeName type="TextString" value="x-ID"/>
0164	<AttributeValue type="TextString" value="TC-312-12-from-
	template"/>
0165	</Attribute>
0166	<Attribute>
0167	<AttributeName type="TextString" value="x-ID"/>
0168	<AttributeIndex type="Integer" value="1"/>
0169	<AttributeValue type="TextString" value="TC-312-12-from-
	create"/>
0170	</Attribute>
0171	<Attribute>
0172	<AttributeName type="TextString" value="x-Purpose"/>
0173	<AttributeValue type="TextString" value="demonstration"/>
0174	</Attribute>
0175	<Attribute>
0176	<AttributeName type="TextString" value="Unique Identifier"/>
0177	<AttributeValue type="TextString"

0178	value="\$UNIQUE_IDENTIFIER_1"/>
0179	</Attribute>
0180	<Attribute type="TextString" value="Object Type"/>
0181	<Attribute value="Enumeration" value="SymmetricKey"/>
0182	</Attribute>
0183	<Attribute
0184	<Attribute type="TextString" value="Cryptographic
	Algorithm"/>
0185	<Attribute value="Enumeration" value="AES"/>
0186	</Attribute>
0187	<Attribute
0188	<Attribute type="TextString" value="Cryptographic
	Length"/>
0189	<Attribute value="Integer" value="128"/>
0190	</Attribute>
0191	<Attribute
0192	<Attribute type="TextString" value="Application Specific
	Information"/>
0193	<Attribute
0194	<ApplicationNamespace type="TextString" value="ssl"/>
0195	<ApplicationData type="TextString"
	value="www.example.com"/>
0196	</Attribute>
0197	</Attribute>
0198	<Attribute
0199	<Attribute type="TextString" value="Contact
	Information"/>
0200	<Attribute value="TextString" value="Joe"/>
0201	</Attribute>
0202	<Attribute
0203	<Attribute type="TextString" value="Cryptographic Usage
	Mask"/>
0204	<Attribute value="Integer" value="Decrypt Encrypt"/>
0205	</Attribute>
0206	<Attribute
0207	<Attribute type="TextString" value="Digest"/>
0208	<Attribute
0209	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0210	<Digest value="ByteString"
	value="c61217ddfa8a8004410ce1a7edd8e5013693a173310918971e146e910d61c
	669"/>
0211	<KeyFormat type="Enumeration" value="Raw"/>
0212	</Attribute>
0213	</Attribute>
0214	<Attribute
0215	<Attribute type="TextString" value="Fresh"/>
0216	<Attribute value="Boolean" value="true"/>
0217	</Attribute>
0218	<Attribute
0219	<Attribute type="TextString" value="Initial Date"/>
0220	<Attribute value="DateTime" value="2013-06-
	17T08:37:31+00:00"/>
0221	</Attribute>
0222	<Attribute
0223	<Attribute type="TextString" value="Last Change Date"/>
0224	<Attribute value="DateTime" value="2013-06-

0225	17T08:37:31+00:00"/>
0226	</Attribute>
0227	<AttributeName type="TextString" value="Lease Time"/>
0228	<AttributeValue type="Interval" value="3600"/>
0229	</Attribute>
0230	<Attribute>
0231	<AttributeName type="TextString" value="Name"/>
0232	<AttributeValue>
0233	<NameValue type="TextString" value="TC-312-12-key1"/>
0234	<NameType type="Enumeration"
0235	value="UninterpretedTextString"/>
0236	</AttributeValue>
0237	</Attribute>
0238	<AttributeName type="TextString" value="Object Group"/>
0239	<AttributeValue type="TextString" value="Group1"/>
0240	</Attribute>
0241	<Attribute>
0242	<AttributeName type="TextString" value="Original Creation
0243	Date"/>
0244	<AttributeValue type="DateTime" value="2013-06-
0245	23T00:11:30+00:00"/>
0246	</Attribute>
0247	<Attribute>
0248	<AttributeName type="TextString" value="State"/>
0249	<AttributeValue type="Enumeration" value="PreActive"/>
0250	</Attribute>
0251	</ResponsePayload>
0252	</BatchItem>
0253	</ResponseMessage>
0254	# TIME 3
0255	<RequestMessage>
0256	<RequestHeader>
0257	<ProtocolVersion>
0258	<ProtocolVersionMajor type="Integer" value="1"/>
0259	<ProtocolVersionMinor type="Integer" value="2"/>
0260	</ProtocolVersion>
0261	<BatchCount type="Integer" value="1"/>
0262	</RequestHeader>
0263	<BatchItem>
0264	<Operation type="Enumeration" value="GetAttributes"/>
0265	<RequestPayload>
0266	<UniqueIdentifier type="TextString"
0267	value="\$UNIQUE_IDENTIFIER_0"/>
0268	</RequestPayload>
0269	</BatchItem>
0270	</RequestMessage>
0271	<ResponseMessage>
0272	<ResponseHeader>
0273	<ProtocolVersion>
0274	<ProtocolVersionMajor type="Integer" value="1"/>
0275	<ProtocolVersionMinor type="Integer" value="2"/>
0276	</ProtocolVersion>
0277	<TimeStamp type="DateTime" value="2013-06-17T08:24:02+00:00"/>
0278	<BatchCount type="Integer" value="1"/>
0279	</ResponseHeader>

0276	<BatchItem>
0277	<Operation type="Enumeration" value="GetAttributes"/>
0278	<ResultStatus type="Enumeration" value="Success"/>
0279	<ResponsePayload>
0280	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0281	<Attribute>
0282	<AttributeName type="TextString" value="x-ID"/>
0283	<AttributeValue type="TextString" value="TC-312-12"/>
0284	</Attribute>
0285	<Attribute>
0286	<AttributeName type="TextString" value="Unique Identifier"/>
0287	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0288	</Attribute>
0289	<Attribute>
0290	<AttributeName type="TextString" value="Object Type"/>
0291	<AttributeValue type="Enumeration" value="Template"/>
0292	</Attribute>
0293	<Attribute>
0294	<AttributeName type="TextString" value="Initial Date"/>
0295	<AttributeValue type="DateTime" value="2013-06-
	17T08:24:02+00:00"/>
0296	</Attribute>
0297	<Attribute>
0298	<AttributeName type="TextString" value="Last Change Date"/>
0299	<AttributeValue type="DateTime" value="2013-06-
	17T08:24:02+00:00"/>
0300	</Attribute>
0301	<Attribute>
0302	<AttributeName type="TextString" value="Lease Time"/>
0303	<AttributeValue type="Interval" value="3600"/>
0304	</Attribute>
0305	<Attribute>
0306	<AttributeName type="TextString" value="Name"/>
0307	<AttributeValue>
0308	<NameValue type="TextString" value="TC-312-12-templatel"/>
0309	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0310	</AttributeValue>
0311	</Attribute>
0312	</ResponsePayload>
0313	</BatchItem>
0314	</ResponseMessage>
# TIME 4	
0315	<RequestMessage>
0316	<RequestHeader>
0317	<ProtocolVersion>
0318	<ProtocolVersionMajor type="Integer" value="1"/>
0319	<ProtocolVersionMinor type="Integer" value="2"/>
0320	</ProtocolVersion>
0321	<BatchCount type="Integer" value="1"/>
0322	</RequestHeader>
0323	<BatchItem>
0324	<Operation type="Enumeration" value="Get"/>
0325	<RequestPayload>
0326	<UniqueIdentifier type="TextString"

0327	value="\$UNIQUE_IDENTIFIER_0"/>
0328	</RequestPayload>
0329	</BatchItem>
0330	</RequestMessage>
0330	<ResponseMessage>
0331	<ResponseHeader>
0332	<ProtocolVersion>
0333	<ProtocolVersionMajor type="Integer" value="1"/>
0334	<ProtocolVersionMinor type="Integer" value="2"/>
0335	</ProtocolVersion>
0336	<TimeStamp type="DateTime" value="2013-06-17T08:40:15+00:00"/>
0337	<BatchCount type="Integer" value="1"/>
0338	</ResponseHeader>
0339	<BatchItem>
0340	<Operation type="Enumeration" value="Get"/>
0341	<ResultStatus type="Enumeration" value="Success"/>
0342	<ResponsePayload>
0343	<ObjectType type="Enumeration" value="Template"/>
0344	<UniqueIdentifier type="TextString" value="8590e6e9-61c1-4b81-98d3-053a3c6a521b"/>
0345	<Template>
0346	<Attribute>
0347	<AttributeName type="TextString" value="Object Group"/>
0348	<AttributeValue type="TextString" value="Group1"/>
0349	</Attribute>
0350	<Attribute>
0351	<AttributeName type="TextString" value="Application Specific Information"/>
0352	<AttributeValue>
0353	<ApplicationNamespace type="TextString" value="ssl"/>
0354	<ApplicationData type="TextString" value="www.example.com"/>
0355	</AttributeValue>
0356	</Attribute>
0357	<Attribute>
0358	<AttributeName type="TextString" value="Contact Information"/>
0359	<AttributeValue type="TextString" value="Joe"/>
0360	</Attribute>
0361	<Attribute>
0362	<AttributeName type="TextString" value="x-Purpose"/>
0363	<AttributeValue type="TextString" value="demonstration"/>
0364	</Attribute>
0365	<Attribute>
0366	<AttributeName type="TextString" value="x-ID"/>
0367	<AttributeValue type="TextString" value="TC-312-12-from-template"/>
0368	</Attribute>
0369	</Template>
0370	</ResponsePayload>
0371	</BatchItem>
0372	</ResponseMessage>
	# TIME 5
0373	<RequestMessage>
0374	<RequestHeader>
0375	<ProtocolVersion>
0376	<ProtocolVersionMajor type="Integer" value="1"/>

0377	<ProtocolVersionMinor type="Integer" value="2"/>
0378	</ProtocolVersion>
0379	<BatchCount type="Integer" value="1"/>
0380	</RequestHeader>
0381	<BatchItem>
0382	<Operation type="Enumeration" value="Destroy"/>
0383	<RequestPayload>
0384	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0385	</RequestPayload>
0386	</BatchItem>
0387	</RequestMessage>
0388	<ResponseMessage>
0389	<ResponseHeader>
0390	<ProtocolVersion>
0391	<ProtocolVersionMajor type="Integer" value="1"/>
0392	<ProtocolVersionMinor type="Integer" value="2"/>
0393	</ProtocolVersion>
0394	<TimeStamp type="DateTime" value="2012-04-27T08:12:22+00:00"/>
0395	<BatchCount type="Integer" value="1"/>
0396	</ResponseHeader>
0397	<BatchItem>
0398	<Operation type="Enumeration" value="Destroy"/>
0399	<ResultStatus type="Enumeration" value="Success"/>
0400	<ResponsePayload>
0401	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0402	</ResponsePayload>
0403	</BatchItem>
0404	</ResponseMessage>
	# TIME 6
0405	<RequestMessage>
0406	<RequestHeader>
0407	<ProtocolVersion>
0408	<ProtocolVersionMajor type="Integer" value="1"/>
0409	<ProtocolVersionMinor type="Integer" value="2"/>
0410	</ProtocolVersion>
0411	<BatchCount type="Integer" value="1"/>
0412	</RequestHeader>
0413	<BatchItem>
0414	<Operation type="Enumeration" value="Destroy"/>
0415	<RequestPayload>
0416	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0417	</RequestPayload>
0418	</BatchItem>
0419	</RequestMessage>
0420	<ResponseMessage>
0421	<ResponseHeader>
0422	<ProtocolVersion>
0423	<ProtocolVersionMajor type="Integer" value="1"/>
0424	<ProtocolVersionMinor type="Integer" value="2"/>
0425	</ProtocolVersion>
0426	<TimeStamp type="DateTime" value="2012-04-27T08:12:22+00:00"/>
0427	<BatchCount type="Integer" value="1"/>
0428	</ResponseHeader>

0429	<BatchItem>
0430	<Operation type="Enumeration" value="Destroy"/>
0431	<ResultStatus type="Enumeration" value="Success"/>
0432	<ResponsePayload>
0433	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0434	</ResponsePayload>
0435	</BatchItem>
0436	</ResponseMessage>

744

745 2.3.3 TC-313-12 - Create / Locate / Get / Destroy

746 This test case tests the Locate and Get operations. A symmetric key is first created, and then a
747 lookup is performed on the Name attribute using the Locate operation. Subsequently, a Get
748 request is issued to retrieve the located key. A locate is performed on the Unique Identifier with
749 State of PreActive (the State the key must be in). The key on the server is destroyed and the
750 locate is performed again which should return no objects (as the state of the key should now be
751 Destroyed).

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Name"/>
0016	<AttributeValue>
0017	<NameValue type="TextString" value="TC-313-12-key1"/>
0018	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0019	</AttributeValue>
0020	</Attribute>
0021	<Attribute>
0022	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0023	<AttributeValue type="Enumeration" value="DES3"/>
0024	</Attribute>
0025	<Attribute>
0026	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0027	<AttributeValue type="Integer" value="168"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>

0031	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="2"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2012-04-27T08:12:22+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
0055	# TIME 1
0056	<RequestMessage>
0057	<RequestHeader>
0058	<ProtocolVersion>
0059	<ProtocolVersionMajor type="Integer" value="1"/>
0060	<ProtocolVersionMinor type="Integer" value="2"/>
0061	</ProtocolVersion>
0062	<BatchCount type="Integer" value="1"/>
0063	</RequestHeader>
0064	<BatchItem>
0065	<Operation type="Enumeration" value="Locate"/>
0066	<RequestPayload>
0067	<Attribute>
0068	<AttributeName type="TextString" value="Object Type"/>
0069	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0070	</Attribute>
0071	<Attribute>
0072	<AttributeName type="TextString" value="Name"/>
0073	<AttributeValue>
0074	<NameValue type="TextString" value="TC-313-12-key1"/>
	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0075	</AttributeValue>
0076	</Attribute>
0077	</RequestPayload>
0078	</BatchItem>
0079	</RequestMessage>
0080	<ResponseMessage>
0081	<ResponseHeader>
0082	<ProtocolVersion>
0083	<ProtocolVersionMajor type="Integer" value="1"/>

0084	<ProtocolVersionMinor type="Integer" value="2"/>
0085	</ProtocolVersion>
0086	<TimeStamp type="DateTime" value="2012-04-27T08:12:22+00:00"/>
0087	<BatchCount type="Integer" value="1"/>
0088	</ResponseHeader>
0089	<BatchItem>
0090	<Operation type="Enumeration" value="Locate"/>
0091	<ResultStatus type="Enumeration" value="Success"/>
0092	<ResponsePayload>
0093	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0094	</ResponsePayload>
0095	</BatchItem>
0096	</ResponseMessage>
# TIME 2	
0097	<RequestMessage>
0098	<RequestHeader>
0099	<ProtocolVersion>
0100	<ProtocolVersionMajor type="Integer" value="1"/>
0101	<ProtocolVersionMinor type="Integer" value="2"/>
0102	</ProtocolVersion>
0103	<BatchCount type="Integer" value="1"/>
0104	</RequestHeader>
0105	<BatchItem>
0106	<Operation type="Enumeration" value="Get"/>
0107	<RequestPayload>
0108	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0109	</RequestPayload>
0110	</BatchItem>
0111	</RequestMessage>
0112	<ResponseMessage>
0113	<ResponseHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="2"/>
0117	</ProtocolVersion>
0118	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0119	<BatchCount type="Integer" value="1"/>
0120	</ResponseHeader>
0121	<BatchItem>
0122	<Operation type="Enumeration" value="Get"/>
0123	<ResultStatus type="Enumeration" value="Success"/>
0124	<ResponsePayload>
0125	<ObjectType type="Enumeration" value="SymmetricKey"/>
0126	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0127	<SymmetricKey>
0128	<KeyBlock>
0129	<KeyFormatType type="Enumeration" value="Raw"/>
0130	<KeyValue>
0131	<KeyMaterial type="ByteString"
	value="7367578051012a6d134a855e25c8cd5e4ca131455729d3c8"/>
0132	</KeyValue>
0133	<CryptographicAlgorithm type="Enumeration" value="DES3"/>
0134	<CryptographicLength type="Integer" value="168"/>
0135	</KeyBlock>

0136	</SymmetricKey>
0137	</ResponsePayload>
0138	</BatchItem>
0139	</ResponseMessage>
# TIME 3	
0140	<RequestMessage>
0141	<RequestHeader>
0142	<ProtocolVersion>
0143	<ProtocolVersionMajor type="Integer" value="1"/>
0144	<ProtocolVersionMinor type="Integer" value="2"/>
0145	</ProtocolVersion>
0146	<BatchCount type="Integer" value="1"/>
0147	</RequestHeader>
0148	<BatchItem>
0149	<Operation type="Enumeration" value="Locate"/>
0150	<RequestPayload>
0151	<Attribute>
0152	<AttributeName type="TextString" value="State"/>
0153	<AttributeValue type="Enumeration" value="PreActive"/>
0154	</Attribute>
0155	<Attribute>
0156	<AttributeName type="TextString" value="Unique Identifier"/>
0157	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0158	</Attribute>
0159	</RequestPayload>
0160	</BatchItem>
0161	</RequestMessage>
0162	<ResponseMessage>
0163	<ResponseHeader>
0164	<ProtocolVersion>
0165	<ProtocolVersionMajor type="Integer" value="1"/>
0166	<ProtocolVersionMinor type="Integer" value="2"/>
0167	</ProtocolVersion>
0168	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0169	<BatchCount type="Integer" value="1"/>
0170	</ResponseHeader>
0171	<BatchItem>
0172	<Operation type="Enumeration" value="Locate"/>
0173	<ResultStatus type="Enumeration" value="Success"/>
0174	<ResponsePayload>
0175	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0176	</ResponsePayload>
0177	</BatchItem>
0178	</ResponseMessage>
# TIME 4	
0179	<RequestMessage>
0180	<RequestHeader>
0181	<ProtocolVersion>
0182	<ProtocolVersionMajor type="Integer" value="1"/>
0183	<ProtocolVersionMinor type="Integer" value="2"/>
0184	</ProtocolVersion>
0185	<BatchCount type="Integer" value="1"/>
0186	</RequestHeader>
0187	<BatchItem>

0188	<Operation type="Enumeration" value="Destroy"/>
0189	<RequestPayload>
0190	<UniqueIdentifier type="TextString"
0191	value="\$UNIQUE_IDENTIFIER_0"/>
0192	</RequestPayload>
0193	</BatchItem>
0194	</RequestMessage>
0194	<ResponseMessage>
0195	<ResponseHeader>
0196	<ProtocolVersion>
0197	<ProtocolVersionMajor type="Integer" value="1"/>
0198	<ProtocolVersionMinor type="Integer" value="2"/>
0199	</ProtocolVersion>
0200	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0201	<BatchCount type="Integer" value="1"/>
0202	</ResponseHeader>
0203	<BatchItem>
0204	<Operation type="Enumeration" value="Destroy"/>
0205	<ResultStatus type="Enumeration" value="Success"/>
0206	<ResponsePayload>
0207	<UniqueIdentifier type="TextString"
0208	value="\$UNIQUE_IDENTIFIER_0"/>
0209	</ResponsePayload>
0210	</BatchItem>
0210	</ResponseMessage>
0211	# TIME 5
0211	<RequestMessage>
0212	<RequestHeader>
0213	<ProtocolVersion>
0214	<ProtocolVersionMajor type="Integer" value="1"/>
0215	<ProtocolVersionMinor type="Integer" value="2"/>
0216	</ProtocolVersion>
0217	<BatchCount type="Integer" value="1"/>
0218	</RequestHeader>
0219	<BatchItem>
0220	<Operation type="Enumeration" value="Locate"/>
0221	<RequestPayload>
0222	<Attribute>
0223	<AttributeName type="TextString" value="State"/>
0224	<AttributeValue type="Enumeration" value="PreActive"/>
0225	</Attribute>
0226	<Attribute>
0227	<AttributeName type="TextString" value="Unique Identifier"/>
0228	<AttributeValue type="TextString"
0229	value="\$UNIQUE_IDENTIFIER_0"/>
0230	</Attribute>
0231	</RequestPayload>
0232	</BatchItem>
0233	</RequestMessage>
0233	<ResponseMessage>
0234	<ResponseHeader>
0235	<ProtocolVersion>
0236	<ProtocolVersionMajor type="Integer" value="1"/>
0237	<ProtocolVersionMinor type="Integer" value="2"/>
0238	</ProtocolVersion>
0239	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>

0240	<BatchCount type="Integer" value="1"/>
0241	</ResponseHeader>
0242	<BatchItem>
0243	<Operation type="Enumeration" value="Locate"/>
0244	<ResultStatus type="Enumeration" value="Success"/>
0245	<ResponsePayload>
0246	</ResponsePayload>
0247	</BatchItem>
0248	</ResponseMessage>

752

753 2.3.4 TC-314-12 - Dual Client Test Case, ID Placeholder-linked Locate & Get 754 Batch

755 This test case has two clients performing operations on the same key. The first client initially
756 registers a template and creates a symmetric key using that template. The second client then
757 does a batched Locate and Get using the ID Placeholder to retrieve the key. The second client
758 thereafter performs a number of operations on the key (Get Attribute List, Get Attribute, Add
759 Attribute, Modify Attribute and Delete Attribute), before the first client finally destroys the key
760 and the template. The first client also tries to Get the key and the template after they have been
761 destroyed, but the Get operation fails in both cases. This test case demonstrates the fact that it
762 is possible for two clients to cooperate and use the same managed object while only having
763 knowledge of a single pre-agreed Name attribute value and without having to share any other
764 information.

	# TIME 0
	# [Client-A]
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="Template"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Name"/>
0016	<AttributeValue>
0017	<NameValue type="TextString" value="TC-314-12-
	template1"/>
0018	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0019	</AttributeValue>
0020	</Attribute>
0021	</TemplateAttribute>
0022	<Template>
0023	<Attribute>
0024	<AttributeName type="TextString" value="Cryptographic

0025	Algorithm"/>
0026	<AttributeValue type="Enumeration" value="AES"/>
0027	</Attribute>
0028	<AttributeName type="TextString" value="Cryptographic
0029	Length"/>
0030	<AttributeValue type="Integer" value="128"/>
0031	</Attribute>
0032	</RequestPayload>
0033	</BatchItem>
0034	</RequestMessage>
0035	<ResponseMessage>
0036	<ResponseHeader>
0037	<ProtocolVersion>
0038	<ProtocolVersionMajor type="Integer" value="1"/>
0039	<ProtocolVersionMinor type="Integer" value="2"/>
0040	</ProtocolVersion>
0041	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0042	<BatchCount type="Integer" value="1"/>
0043	</ResponseHeader>
0044	<BatchItem>
0045	<Operation type="Enumeration" value="Register"/>
0046	<ResultStatus type="Enumeration" value="Success"/>
0047	<ResponsePayload>
0048	<UniqueIdentifier type="TextString"
0049	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
0053	# TIME 1
0054	# [Client-A]
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="2"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="Create"/>
0065	<RequestPayload>
0066	<ObjectType type="Enumeration" value="SymmetricKey"/>
0067	<TemplateAttribute>
0068	<Name>
0069	<NameValue type="TextString" value="TC-314-12-templatel"/>
0070	<NameType type="Enumeration"
0071	value="UninterpretedTextString"/>
0072	</Name>
0073	<Attribute>
0074	<AttributeName type="TextString" value="Name"/>
	<AttributeValue>
	<NameValue type="TextString" value="TC-314-12-key1"/>
	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
	</Attribute>

0075	</Attribute>
0076	<Attribute>
0077	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0078	<AttributeValue type="Integer" value="Encrypt"/>
0079	</Attribute>
0080	<Attribute>
0081	<AttributeName type="TextString" value="Contact Information"/>
0082	<AttributeValue type="TextString" value="Foo"/>
0083	</Attribute>
0084	</TemplateAttribute>
0085	</RequestPayload>
0086	</BatchItem>
0087	</RequestMessage>
0088	<ResponseMessage>
0089	<ResponseHeader>
0090	<ProtocolVersion>
0091	<ProtocolVersionMajor type="Integer" value="1"/>
0092	<ProtocolVersionMinor type="Integer" value="2"/>
0093	</ProtocolVersion>
0094	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0095	<BatchCount type="Integer" value="1"/>
0096	</ResponseHeader>
0097	<BatchItem>
0098	<Operation type="Enumeration" value="Create"/>
0099	<ResultStatus type="Enumeration" value="Success"/>
0100	<ResponsePayload>
0101	<ObjectType type="Enumeration" value="SymmetricKey"/>
0102	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0103	</ResponsePayload>
0104	</BatchItem>
0105	</ResponseMessage>
	# TIME 2
	# [Client-B]
0106	<RequestMessage>
0107	<RequestHeader>
0108	<ProtocolVersion>
0109	<ProtocolVersionMajor type="Integer" value="1"/>
0110	<ProtocolVersionMinor type="Integer" value="2"/>
0111	</ProtocolVersion>
0112	<BatchOrderOption type="Boolean" value="true"/>
0113	<BatchCount type="Integer" value="2"/>
0114	</RequestHeader>
0115	<BatchItem>
0116	<Operation type="Enumeration" value="Locate"/>
0117	<UniqueBatchItemID type="ByteString" value="aa21f8c659d6e10d"/>
0118	<RequestPayload>
0119	<Attribute>
0120	<AttributeName type="TextString" value="Object Type"/>
0121	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0122	</Attribute>
0123	<Attribute>
0124	<AttributeName type="TextString" value="Name"/>
0125	<AttributeValue>
0126	<NameValue type="TextString" value="TC-314-12-key1"/>

0127	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0128	</AttributeValue>
0129	</Attribute>
0130	</RequestPayload>
0131	</BatchItem>
0132	<BatchItem>
0133	<Operation type="Enumeration" value="Get"/>
0134	<UniqueBatchItemID type="ByteString" value="495a95f165854dle"/>
0135	<RequestPayload>
0136	</RequestPayload>
0137	</BatchItem>
0138	</RequestMessage>
0139	<ResponseMessage>
0140	<ResponseHeader>
0141	<ProtocolVersion>
0142	<ProtocolVersionMajor type="Integer" value="1"/>
0143	<ProtocolVersionMinor type="Integer" value="2"/>
0144	</ProtocolVersion>
0145	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0146	<BatchCount type="Integer" value="2"/>
0147	</ResponseHeader>
0148	<BatchItem>
0149	<Operation type="Enumeration" value="Locate"/>
0150	<UniqueBatchItemID type="ByteString" value="aa21f8c659d6e10d"/>
0151	<ResultStatus type="Enumeration" value="Success"/>
0152	<ResponsePayload>
0153	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0154	</ResponsePayload>
0155	</BatchItem>
0156	<BatchItem>
0157	<Operation type="Enumeration" value="Get"/>
0158	<UniqueBatchItemID type="ByteString" value="495a95f165854dle"/>
0159	<ResultStatus type="Enumeration" value="Success"/>
0160	<ResponsePayload>
0161	<ObjectType type="Enumeration" value="SymmetricKey"/>
0162	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0163	<SymmetricKey>
0164	<KeyBlock>
0165	<KeyFormatType type="Enumeration" value="Raw"/>
0166	<KeyValue>
0167	<KeyMaterial type="ByteString"
	value="d351910f1d7934d6e2ae17576564e2bc"/>
0168	</KeyValue>
0169	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0170	<CryptographicLength type="Integer" value="128"/>
0171	</KeyBlock>
0172	</SymmetricKey>
0173	</ResponsePayload>
0174	</BatchItem>
0175	</ResponseMessage>
	# TIME 3
	# [Client-B]
0176	<RequestMessage>
0177	<RequestHeader>

0178	<ProtocolVersion>
0179	<ProtocolVersionMajor type="Integer" value="1"/>
0180	<ProtocolVersionMinor type="Integer" value="2"/>
0181	</ProtocolVersion>
0182	<BatchCount type="Integer" value="1"/>
0183	</RequestHeader>
0184	<BatchItem>
0185	<Operation type="Enumeration" value="GetAttributeList"/>
0186	<RequestPayload>
0187	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0188	</RequestPayload>
0189	</BatchItem>
0190	</RequestMessage>
0191	<ResponseMessage>
0192	<ResponseHeader>
0193	<ProtocolVersion>
0194	<ProtocolVersionMajor type="Integer" value="1"/>
0195	<ProtocolVersionMinor type="Integer" value="2"/>
0196	</ProtocolVersion>
0197	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0198	<BatchCount type="Integer" value="1"/>
0199	</ResponseHeader>
0200	<BatchItem>
0201	<Operation type="Enumeration" value="GetAttributeList"/>
0202	<ResultStatus type="Enumeration" value="Success"/>
0203	<ResponsePayload>
0204	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0205	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0206	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0207	<AttributeName type="TextString" value="State"/>
0208	<AttributeName type="TextString" value="Digest"/>
0209	<AttributeName type="TextString" value="Lease Time"/>
0210	<AttributeName type="TextString" value="Initial Date"/>
0211	<AttributeName type="TextString" value="Unique Identifier"/>
0212	<AttributeName type="TextString" value="Name"/>
0213	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0214	<AttributeName type="TextString" value="Object Type"/>
0215	<AttributeName type="TextString" value="Contact Information"/>
0216	<AttributeName type="TextString" value="Last Change Date"/>
0217	<AttributeName type="TextString" value="Original Creation
	Date"/>
0218	<AttributeName type="TextString" value="Fresh"/>
0219	</ResponsePayload>
0220	</BatchItem>
0221	</ResponseMessage>
	# TIME 4
	# [Client-B]
0222	<RequestMessage>
0223	<RequestHeader>
0224	<ProtocolVersion>
0225	<ProtocolVersionMajor type="Integer" value="1"/>
0226	<ProtocolVersionMinor type="Integer" value="2"/>

0227	</ProtocolVersion>
0228	<BatchCount type="Integer" value="1"/>
0229	</RequestHeader>
0230	<BatchItem>
0231	<Operation type="Enumeration" value="GetAttributes"/>
0232	<RequestPayload>
0233	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0234	<AttributeName type="TextString" value="Name"/>
0235	<AttributeName type="TextString" value="Contact Information"/>
0236	</RequestPayload>
0237	</BatchItem>
0238	</RequestMessage>
0239	<ResponseMessage>
0240	<ResponseHeader>
0241	<ProtocolVersion>
0242	<ProtocolVersionMajor type="Integer" value="1"/>
0243	<ProtocolVersionMinor type="Integer" value="2"/>
0244	</ProtocolVersion>
0245	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0246	<BatchCount type="Integer" value="1"/>
0247	</ResponseHeader>
0248	<BatchItem>
0249	<Operation type="Enumeration" value="GetAttributes"/>
0250	<ResultStatus type="Enumeration" value="Success"/>
0251	<ResponsePayload>
0252	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0253	<Attribute>
0254	<AttributeName type="TextString" value="Name"/>
0255	<AttributeValue>
0256	<NameValue type="TextString" value="TC-314-12-key1"/>
0257	<NameType type="Enumeration" value="UninterpretedTextString"/>
0258	</AttributeValue>
0259	</Attribute>
0260	<Attribute>
0261	<AttributeName type="TextString" value="Contact Information"/>
0262	<AttributeValue type="TextString" value="Foo"/>
0263	</Attribute>
0264	</ResponsePayload>
0265	</BatchItem>
0266	</ResponseMessage>
	# TIME 5
	# [Client-B]
0267	<RequestMessage>
0268	<RequestHeader>
0269	<ProtocolVersion>
0270	<ProtocolVersionMajor type="Integer" value="1"/>
0271	<ProtocolVersionMinor type="Integer" value="2"/>
0272	</ProtocolVersion>
0273	<BatchCount type="Integer" value="2"/>
0274	</RequestHeader>
0275	<BatchItem>
0276	<Operation type="Enumeration" value="AddAttribute"/>
0277	<UniqueBatchItemID type="ByteString" value="32d84369c120488e"/>

0278	<RequestPayload>
0279	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0280	<Attribute>
0281	<AttributeName type="TextString" value="x-attribute1"/>
0282	<AttributeValue type="TextString" value="Value1"/>
0283	</Attribute>
0284	</RequestPayload>
0285	</BatchItem>
0286	<BatchItem>
0287	<Operation type="Enumeration" value="AddAttribute"/>
0288	<UniqueBatchItemID type="ByteString" value="519cf4f0eclac13f"/>
0289	<RequestPayload>
0290	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0291	<Attribute>
0292	<AttributeName type="TextString" value="x-attribute2"/>
0293	<AttributeValue type="TextString" value="Value2"/>
0294	</Attribute>
0295	</RequestPayload>
0296	</BatchItem>
0297	</RequestMessage>
0298	<ResponseMessage>
0299	<ResponseHeader>
0300	<ProtocolVersion>
0301	<ProtocolVersionMajor type="Integer" value="1"/>
0302	<ProtocolVersionMinor type="Integer" value="2"/>
0303	</ProtocolVersion>
0304	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0305	<BatchCount type="Integer" value="2"/>
0306	</ResponseHeader>
0307	<BatchItem>
0308	<Operation type="Enumeration" value="AddAttribute"/>
0309	<UniqueBatchItemID type="ByteString" value="32d84369c120488e"/>
0310	<ResultStatus type="Enumeration" value="Success"/>
0311	<ResponsePayload>
0312	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0313	<Attribute>
0314	<AttributeName type="TextString" value="x-attribute1"/>
0315	<AttributeValue type="TextString" value="Value1"/>
0316	</Attribute>
0317	</ResponsePayload>
0318	</BatchItem>
0319	<BatchItem>
0320	<Operation type="Enumeration" value="AddAttribute"/>
0321	<UniqueBatchItemID type="ByteString" value="519cf4f0eclac13f"/>
0322	<ResultStatus type="Enumeration" value="Success"/>
0323	<ResponsePayload>
0324	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0325	<Attribute>
0326	<AttributeName type="TextString" value="x-attribute2"/>
0327	<AttributeValue type="TextString" value="Value2"/>
0328	</Attribute>
0329	</ResponsePayload>
0330	</BatchItem>

0331	</ResponseMessage>
	# TIME 6
	# [Client-B]
0332	<RequestMessage>
0333	<RequestHeader>
0334	<ProtocolVersion>
0335	<ProtocolVersionMajor type="Integer" value="1"/>
0336	<ProtocolVersionMinor type="Integer" value="2"/>
0337	</ProtocolVersion>
0338	<BatchCount type="Integer" value="2"/>
0339	</RequestHeader>
0340	<BatchItem>
0341	<Operation type="Enumeration" value="ModifyAttribute"/>
0342	<UniqueBatchItemID type="ByteString" value="fce08e45995686b6"/>
0343	<RequestPayload>
0344	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0345	<Attribute>
0346	<AttributeName type="TextString" value="x-attribute1"/>
0347	<AttributeValue type="TextString" value="ModifiedValue1"/>
0348	</Attribute>
0349	</RequestPayload>
0350	</BatchItem>
0351	<BatchItem>
0352	<Operation type="Enumeration" value="ModifyAttribute"/>
0353	<UniqueBatchItemID type="ByteString" value="dc2bfda88f39f5fc"/>
0354	<RequestPayload>
0355	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0356	<Attribute>
0357	<AttributeName type="TextString" value="x-attribute2"/>
0358	<AttributeValue type="TextString" value="ModifiedValue2"/>
0359	</Attribute>
0360	</RequestPayload>
0361	</BatchItem>
0362	</RequestMessage>
0363	<ResponseMessage>
0364	<ResponseHeader>
0365	<ProtocolVersion>
0366	<ProtocolVersionMajor type="Integer" value="1"/>
0367	<ProtocolVersionMinor type="Integer" value="2"/>
0368	</ProtocolVersion>
0369	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0370	<BatchCount type="Integer" value="2"/>
0371	</ResponseHeader>
0372	<BatchItem>
0373	<Operation type="Enumeration" value="ModifyAttribute"/>
0374	<UniqueBatchItemID type="ByteString" value="fce08e45995686b6"/>
0375	<ResultStatus type="Enumeration" value="Success"/>
0376	<ResponsePayload>
0377	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0378	<Attribute>
0379	<AttributeName type="TextString" value="x-attribute1"/>
0380	<AttributeValue type="TextString" value="ModifiedValue1"/>
0381	</Attribute>
0382	</ResponsePayload>

0383	</BatchItem>
0384	<BatchItem>
0385	<Operation type="Enumeration" value="ModifyAttribute"/>
0386	<UniqueBatchItemID type="ByteString" value="dc2bfda88f39f5fc"/>
0387	<ResultStatus type="Enumeration" value="Success"/>
0388	<ResponsePayload>
0389	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0390	<Attribute>
0391	<AttributeName type="TextString" value="x-attribute2"/>
0392	<AttributeValue type="TextString" value="ModifiedValue2"/>
0393	</Attribute>
0394	</ResponsePayload>
0395	</BatchItem>
0396	</ResponseMessage>
	# TIME 7
	# [Client-B]
0397	<RequestMessage>
0398	<RequestHeader>
0399	<ProtocolVersion>
0400	<ProtocolVersionMajor type="Integer" value="1"/>
0401	<ProtocolVersionMinor type="Integer" value="2"/>
0402	</ProtocolVersion>
0403	<BatchCount type="Integer" value="2"/>
0404	</RequestHeader>
0405	<BatchItem>
0406	<Operation type="Enumeration" value="DeleteAttribute"/>
0407	<UniqueBatchItemID type="ByteString" value="ba8d4889753b7414"/>
0408	<RequestPayload>
0409	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0410	<AttributeName type="TextString" value="x-attribute1"/>
0411	</RequestPayload>
0412	</BatchItem>
0413	<BatchItem>
0414	<Operation type="Enumeration" value="DeleteAttribute"/>
0415	<UniqueBatchItemID type="ByteString" value="88fa2f142c615edb"/>
0416	<RequestPayload>
0417	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0418	<AttributeName type="TextString" value="x-attribute2"/>
0419	</RequestPayload>
0420	</BatchItem>
0421	</RequestMessage>
0422	<ResponseMessage>
0423	<ResponseHeader>
0424	<ProtocolVersion>
0425	<ProtocolVersionMajor type="Integer" value="1"/>
0426	<ProtocolVersionMinor type="Integer" value="2"/>
0427	</ProtocolVersion>
0428	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0429	<BatchCount type="Integer" value="2"/>
0430	</ResponseHeader>
0431	<BatchItem>
0432	<Operation type="Enumeration" value="DeleteAttribute"/>
0433	<UniqueBatchItemID type="ByteString" value="ba8d4889753b7414"/>
0434	<ResultStatus type="Enumeration" value="Success"/>

0435	<ResponsePayload>
0436	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0437	<Attribute>
0438	<AttributeName type="TextString" value="x-attribute1"/>
0439	<AttributeValue type="TextString" value="ModifiedValue1"/>
0440	</Attribute>
0441	</ResponsePayload>
0442	</BatchItem>
0443	<BatchItem>
0444	<Operation type="Enumeration" value="DeleteAttribute"/>
0445	<UniqueBatchItemID type="ByteString" value="88fa2f142c615edb"/>
0446	<ResultStatus type="Enumeration" value="Success"/>
0447	<ResponsePayload>
0448	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0449	<Attribute>
0450	<AttributeName type="TextString" value="x-attribute2"/>
0451	<AttributeValue type="TextString" value="ModifiedValue2"/>
0452	</Attribute>
0453	</ResponsePayload>
0454	</BatchItem>
0455	</ResponseMessage>
	# TIME 8
	# [Client-A]
0456	<RequestMessage>
0457	<RequestHeader>
0458	<ProtocolVersion>
0459	<ProtocolVersionMajor type="Integer" value="1"/>
0460	<ProtocolVersionMinor type="Integer" value="2"/>
0461	</ProtocolVersion>
0462	<BatchCount type="Integer" value="1"/>
0463	</RequestHeader>
0464	<BatchItem>
0465	<Operation type="Enumeration" value="Destroy"/>
0466	<RequestPayload>
0467	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0468	</RequestPayload>
0469	</BatchItem>
0470	</RequestMessage>
0471	<ResponseMessage>
0472	<ResponseHeader>
0473	<ProtocolVersion>
0474	<ProtocolVersionMajor type="Integer" value="1"/>
0475	<ProtocolVersionMinor type="Integer" value="2"/>
0476	</ProtocolVersion>
0477	<TimeStamp type="DateTime" value="2012-04-27T08:12:23+00:00"/>
0478	<BatchCount type="Integer" value="1"/>
0479	</ResponseHeader>
0480	<BatchItem>
0481	<Operation type="Enumeration" value="Destroy"/>
0482	<ResultStatus type="Enumeration" value="Success"/>
0483	<ResponsePayload>
0484	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0485	</ResponsePayload>

0486	</BatchItem>
0487	</ResponseMessage>
0488	# TIME 9
0489	# [Client-A]
0488	<RequestMessage>
0489	<RequestHeader>
0490	<ProtocolVersion>
0491	<ProtocolVersionMajor type="Integer" value="1"/>
0492	<ProtocolVersionMinor type="Integer" value="2"/>
0493	</ProtocolVersion>
0494	<BatchCount type="Integer" value="1"/>
0495	</RequestHeader>
0496	<BatchItem>
0497	<Operation type="Enumeration" value="Get"/>
0498	<RequestPayload>
0499	<UniqueIdentifier type="TextString"
0500	value="\$UNIQUE_IDENTIFIER_1"/>
0501	</RequestPayload>
0502	</BatchItem>
0503	</RequestMessage>
0504	<ResponseMessage>
0505	<ResponseHeader>
0506	<ProtocolVersion>
0507	<ProtocolVersionMajor type="Integer" value="1"/>
0508	<ProtocolVersionMinor type="Integer" value="2"/>
0509	</ProtocolVersion>
0510	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0511	<BatchCount type="Integer" value="1"/>
0512	</ResponseHeader>
0513	<BatchItem>
0514	<Operation type="Enumeration" value="Get"/>
0515	<ResultStatus type="Enumeration" value="OperationFailed"/>
0516	<ResultReason type="Enumeration" value="ItemNotFound"/>
0517	<ResultMessage type="TextString" value="No Cryptographic Object
0518	found with given Unique Identifier"/>
0519	</BatchItem>
0520	</ResponseMessage>
0521	# TIME 10
0522	# [Client-A]
0523	<RequestMessage>
0524	<RequestHeader>
0525	<ProtocolVersion>
0526	<ProtocolVersionMajor type="Integer" value="1"/>
0527	<ProtocolVersionMinor type="Integer" value="2"/>
0528	</ProtocolVersion>
0529	<BatchCount type="Integer" value="1"/>
0530	</RequestHeader>
0531	<BatchItem>
0532	<Operation type="Enumeration" value="Destroy"/>
0533	<RequestPayload>
0534	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
	</RequestPayload>
	</BatchItem>
	</RequestMessage>
	<ResponseMessage>

0535	<ResponseHeader>
0536	<ProtocolVersion>
0537	<ProtocolVersionMajor type="Integer" value="1"/>
0538	<ProtocolVersionMinor type="Integer" value="2"/>
0539	</ProtocolVersion>
0540	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0541	<BatchCount type="Integer" value="1"/>
0542	</ResponseHeader>
0543	<BatchItem>
0544	<Operation type="Enumeration" value="Destroy"/>
0545	<ResultStatus type="Enumeration" value="Success"/>
0546	<ResponsePayload>
0547	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0548	</ResponsePayload>
0549	</BatchItem>
0550	</ResponseMessage>
	# TIME 11
	# [Client-A]
0551	<RequestMessage>
0552	<RequestHeader>
0553	<ProtocolVersion>
0554	<ProtocolVersionMajor type="Integer" value="1"/>
0555	<ProtocolVersionMinor type="Integer" value="2"/>
0556	</ProtocolVersion>
0557	<BatchCount type="Integer" value="1"/>
0558	</RequestHeader>
0559	<BatchItem>
0560	<Operation type="Enumeration" value="Get"/>
0561	<RequestPayload>
0562	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0563	</RequestPayload>
0564	</BatchItem>
0565	</RequestMessage>
0566	<ResponseMessage>
0567	<ResponseHeader>
0568	<ProtocolVersion>
0569	<ProtocolVersionMajor type="Integer" value="1"/>
0570	<ProtocolVersionMinor type="Integer" value="2"/>
0571	</ProtocolVersion>
0572	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0573	<BatchCount type="Integer" value="1"/>
0574	</ResponseHeader>
0575	<BatchItem>
0576	<Operation type="Enumeration" value="Get"/>
0577	<ResultStatus type="Enumeration" value="OperationFailed"/>
0578	<ResultReason type="Enumeration" value="ItemNotFound"/>
0579	<ResultMessage type="TextString" value="No Cryptographic Object
	found with given Unique Identifier"/>
0580	</BatchItem>
0581	</ResponseMessage>

765

766 2.3.5 TC-315-12 - Register / Destroy Secret Data

767 In this test case the client issues a Register request containing a Secret Data object, whereby the
768 server registers the object and returns the Unique Identifier. To clean up, the client then
769 performs a Destroy

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SecretData"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Verify"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-315-12"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<SecretData>
0024	<SecretDataType type="Enumeration" value="Password"/>
0025	<KeyBlock>
0026	<KeyFormatType type="Enumeration" value="Opaque"/>
0027	<KeyValue>
0028	<KeyMaterial type="ByteString" value="53656372657450617373776f7264"/>
0029	</KeyValue>
0030	</KeyBlock>
0031	</SecretData>
0032	</RequestPayload>
0033	</BatchItem>
0034	</RequestMessage>
0035	<ResponseMessage>
0036	<ResponseHeader>
0037	<ProtocolVersion>
0038	<ProtocolVersionMajor type="Integer" value="1"/>
0039	<ProtocolVersionMinor type="Integer" value="2"/>
0040	</ProtocolVersion>
0041	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0042	<BatchCount type="Integer" value="1"/>
0043	</ResponseHeader>
0044	<BatchItem>
0045	<Operation type="Enumeration" value="Register"/>
0046	<ResultStatus type="Enumeration" value="Success"/>
0047	<ResponsePayload>

0048	<UniqueIdentifier type="TextString"
0049	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
0052	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="2"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Destroy"/>
0063	<RequestPayload>
0064	<UniqueIdentifier type="TextString"
0065	value="\$UNIQUE_IDENTIFIER_0"/>
0066	</RequestPayload>
0067	</BatchItem>
0068	</RequestMessage>
0069	<ResponseMessage>
0070	<ResponseHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="2"/>
0074	</ProtocolVersion>
0075	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0076	<BatchCount type="Integer" value="1"/>
0077	</ResponseHeader>
0078	<BatchItem>
0079	<Operation type="Enumeration" value="Destroy"/>
0080	<ResultStatus type="Enumeration" value="Success"/>
0081	<ResponsePayload>
0082	<UniqueIdentifier type="TextString"
0083	value="\$UNIQUE_IDENTIFIER_0"/>
	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>

770

771 2.3.6 TC-32-12 - Asynchronous Locate

772 This test case tests the asynchronous capabilities of KMIP using the Locate operation. A key is
773 created and then a Locate request is sent containing the Name of the created key and with the
774 message header Asynchronous Indicator-field set to True. If the server returns an asynchronous
775 response to the Locate, the client then polls the server until the operation is ready. If the server
776 responded asynchronously, a subsequent Locate operation that is also handled asynchronously
777 is then Canceled, before the key is finally destroyed.

778 This test case shows the use of two clients. Since the client is unable to force the server to
779 respond asynchronously, it is possible for a server to respond synchronously to the requests
780 issued at times 1 and 4, in which case the expected responses are the ones shown at times 2

781 and 5, respectively. In the case of the server not responding asynchronously to the Locate
782 requests, the client is permitted to skip the requests illustrated at time 7 and 8.

783 Note: a server may perform all operations synchronously and not require the use of Poll for the
784 client to wait for the operations to complete

	# TIME 0
	# [Client-A]
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Name"/>
0024	<AttributeValue>
0025	<NameValue type="TextString" value="TC-32-12-key1"/>
0026	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0027	</AttributeValue>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0031	<AttributeValue type="Integer" value="Encrypt"/>
0032	</Attribute>
0033	<Attribute>
0034	<AttributeName type="TextString" value="Object Group"/>
0035	<AttributeValue type="TextString" value="Group1"/>
0036	</Attribute>
0037	</TemplateAttribute>
0038	</RequestPayload>
0039	</BatchItem>
0040	</RequestMessage>
0041	<ResponseMessage>
0042	<ResponseHeader>
0043	<ProtocolVersion>
0044	<ProtocolVersionMajor type="Integer" value="1"/>

0045	<ProtocolVersionMinor type="Integer" value="2"/>
0046	</ProtocolVersion>
0047	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0048	<BatchCount type="Integer" value="1"/>
0049	</ResponseHeader>
0050	<BatchItem>
0051	<Operation type="Enumeration" value="Create"/>
0052	<ResultStatus type="Enumeration" value="Success"/>
0053	<ResponsePayload>
0054	<ObjectType type="Enumeration" value="SymmetricKey"/>
0055	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0056	</ResponsePayload>
0057	</BatchItem>
0058	</ResponseMessage>
	# TIME 1
	# [Client-B]
0059	<RequestMessage>
0060	<RequestHeader>
0061	<ProtocolVersion>
0062	<ProtocolVersionMajor type="Integer" value="1"/>
0063	<ProtocolVersionMinor type="Integer" value="2"/>
0064	</ProtocolVersion>
0065	<AsynchronousIndicator type="Boolean" value="true"/>
0066	<BatchCount type="Integer" value="1"/>
0067	</RequestHeader>
0068	<BatchItem>
0069	<Operation type="Enumeration" value="Locate"/>
0070	<RequestPayload>
0071	<Attribute>
0072	<AttributeName type="TextString" value="Object Type"/>
0073	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0074	</Attribute>
0075	<Attribute>
0076	<AttributeName type="TextString" value="Name"/>
0077	<AttributeValue>
0078	<NameValue type="TextString" value="TC-32-12-key1"/>
0079	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0080	</AttributeValue>
0081	</Attribute>
0082	</RequestPayload>
0083	</BatchItem>
0084	</RequestMessage>
0085	<ResponseMessage>
0086	<ResponseHeader>
0087	<ProtocolVersion>
0088	<ProtocolVersionMajor type="Integer" value="1"/>
0089	<ProtocolVersionMinor type="Integer" value="2"/>
0090	</ProtocolVersion>
0091	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0092	<BatchCount type="Integer" value="1"/>
0093	</ResponseHeader>
0094	<BatchItem>
0095	<Operation type="Enumeration" value="Locate"/>
0096	<ResultStatus type="Enumeration" value="OperationPending"/>
0097	<AsynchronousCorrelationValue type="ByteString"

0098	<code>value="\$ASYNCHRONOUS_CORRELATION_VALUE"/></code>
0099	<code></BatchItem></code>
	<code></ResponseMessage></code>
	<code># TIME 2</code>
	<code># [Client-B]</code>
	<code># [REPEAT] until Locate response is returned</code>
0100	<code><RequestMessage></code>
0101	<code><RequestHeader></code>
0102	<code><ProtocolVersion></code>
0103	<code><ProtocolVersionMajor type="Integer" value="1"/></code>
0104	<code><ProtocolVersionMinor type="Integer" value="2"/></code>
0105	<code></ProtocolVersion></code>
0106	<code><BatchCount type="Integer" value="1"/></code>
0107	<code></RequestHeader></code>
0108	<code><BatchItem></code>
0109	<code><Operation type="Enumeration" value="Poll"/></code>
0110	<code><RequestPayload></code>
0111	<code><AsynchronousCorrelationValue type="ByteString"</code>
	<code>value="\$ASYNCHRONOUS_CORRELATION_VALUE"/></code>
0112	<code></RequestPayload></code>
0113	<code></BatchItem></code>
0114	<code></RequestMessage></code>
0115	<code><ResponseMessage></code>
0116	<code><ResponseHeader></code>
0117	<code><ProtocolVersion></code>
0118	<code><ProtocolVersionMajor type="Integer" value="1"/></code>
0119	<code><ProtocolVersionMinor type="Integer" value="2"/></code>
0120	<code></ProtocolVersion></code>
0121	<code><TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/></code>
0122	<code><BatchCount type="Integer" value="1"/></code>
0123	<code></ResponseHeader></code>
0124	<code><BatchItem></code>
0125	<code><Operation type="Enumeration" value="Locate"/></code>
0126	<code><ResultStatus type="Enumeration" value="Success"/></code>
0127	<code><ResponsePayload></code>
0128	<code><UniqueIdentifier type="TextString"</code>
	<code>value="\$UNIQUE_IDENTIFIER_0"/></code>
0129	<code></ResponsePayload></code>
0130	<code></BatchItem></code>
0131	<code></ResponseMessage></code>
	<code># TIME 3</code>
	<code># [Client-B]</code>
0132	<code><RequestMessage></code>
0133	<code><RequestHeader></code>
0134	<code><ProtocolVersion></code>
0135	<code><ProtocolVersionMajor type="Integer" value="1"/></code>
0136	<code><ProtocolVersionMinor type="Integer" value="2"/></code>
0137	<code></ProtocolVersion></code>
0138	<code><BatchCount type="Integer" value="1"/></code>
0139	<code></RequestHeader></code>
0140	<code><BatchItem></code>
0141	<code><Operation type="Enumeration" value="Get"/></code>
0142	<code><RequestPayload></code>
0143	<code><UniqueIdentifier type="TextString"</code>
	<code>value="\$UNIQUE_IDENTIFIER_0"/></code>
0144	<code></RequestPayload></code>

0145	</BatchItem>
0146	</RequestMessage>
0147	<ResponseMessage>
0148	<ResponseHeader>
0149	<ProtocolVersion>
0150	<ProtocolVersionMajor type="Integer" value="1"/>
0151	<ProtocolVersionMinor type="Integer" value="2"/>
0152	</ProtocolVersion>
0153	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0154	<BatchCount type="Integer" value="1"/>
0155	</ResponseHeader>
0156	<BatchItem>
0157	<Operation type="Enumeration" value="Get"/>
0158	<ResultStatus type="Enumeration" value="Success"/>
0159	<ResponsePayload>
0160	<ObjectType type="Enumeration" value="SymmetricKey"/>
0161	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0162	<SymmetricKey>
0163	<KeyBlock>
0164	<KeyFormatType type="Enumeration" value="Raw"/>
0165	<KeyValue>
0166	<KeyMaterial type="ByteString"
	value="cc9e3b20f5c4fc4d1298f68d0b7de65b"/>
0167	</KeyValue>
0168	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0169	<CryptographicLength type="Integer" value="128"/>
0170	</KeyBlock>
0171	</SymmetricKey>
0172	</ResponsePayload>
0173	</BatchItem>
0174	</ResponseMessage>
	# TIME 4
	# [Client-B]
0175	<RequestMessage>
0176	<RequestHeader>
0177	<ProtocolVersion>
0178	<ProtocolVersionMajor type="Integer" value="1"/>
0179	<ProtocolVersionMinor type="Integer" value="2"/>
0180	</ProtocolVersion>
0181	<AsynchronousIndicator type="Boolean" value="true"/>
0182	<BatchCount type="Integer" value="1"/>
0183	</RequestHeader>
0184	<BatchItem>
0185	<Operation type="Enumeration" value="Locate"/>
0186	<RequestPayload>
0187	<Attribute>
0188	<AttributeName type="TextString" value="Object Type"/>
0189	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0190	</Attribute>
0191	<Attribute>
0192	<AttributeName type="TextString" value="Object Group"/>
0193	<AttributeValue type="TextString" value="Group1"/>
0194	</Attribute>
0195	</RequestPayload>
0196	</BatchItem>
0197	</RequestMessage>

0198	<ResponseMessage>
0199	<ResponseHeader>
0200	<ProtocolVersion>
0201	<ProtocolVersionMajor type="Integer" value="1"/>
0202	<ProtocolVersionMinor type="Integer" value="2"/>
0203	</ProtocolVersion>
0204	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0205	<BatchCount type="Integer" value="1"/>
0206	</ResponseHeader>
0207	<BatchItem>
0208	<Operation type="Enumeration" value="Locate"/>
0209	<ResultStatus type="Enumeration" value="OperationPending"/>
0210	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0211	</BatchItem>
0212	</ResponseMessage>
	# TIME 5
	# [Client-B]
	# [REPEAT] until Locate response is returned
0213	<RequestMessage>
0214	<RequestHeader>
0215	<ProtocolVersion>
0216	<ProtocolVersionMajor type="Integer" value="1"/>
0217	<ProtocolVersionMinor type="Integer" value="2"/>
0218	</ProtocolVersion>
0219	<BatchCount type="Integer" value="1"/>
0220	</RequestHeader>
0221	<BatchItem>
0222	<Operation type="Enumeration" value="Poll"/>
0223	<RequestPayload>
0224	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0225	</RequestPayload>
0226	</BatchItem>
0227	</RequestMessage>
0228	<ResponseMessage>
0229	<ResponseHeader>
0230	<ProtocolVersion>
0231	<ProtocolVersionMajor type="Integer" value="1"/>
0232	<ProtocolVersionMinor type="Integer" value="2"/>
0233	</ProtocolVersion>
0234	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0235	<BatchCount type="Integer" value="1"/>
0236	</ResponseHeader>
0237	<BatchItem>
0238	<Operation type="Enumeration" value="Locate"/>
0239	<ResultStatus type="Enumeration" value="Success"/>
0240	<ResponsePayload>
0241	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0242	</ResponsePayload>
0243	</BatchItem>
0244	</ResponseMessage>
	# TIME 6
	# [Client-B]
0245	<RequestMessage>

0246	<RequestHeader>
0247	<ProtocolVersion>
0248	<ProtocolVersionMajor type="Integer" value="1"/>
0249	<ProtocolVersionMinor type="Integer" value="2"/>
0250	</ProtocolVersion>
0251	<BatchCount type="Integer" value="1"/>
0252	</RequestHeader>
0253	<BatchItem>
0254	<Operation type="Enumeration" value="Get"/>
0255	<RequestPayload>
0256	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0257	</RequestPayload>
0258	</BatchItem>
0259	</RequestMessage>
0260	<ResponseMessage>
0261	<ResponseHeader>
0262	<ProtocolVersion>
0263	<ProtocolVersionMajor type="Integer" value="1"/>
0264	<ProtocolVersionMinor type="Integer" value="2"/>
0265	</ProtocolVersion>
0266	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0267	<BatchCount type="Integer" value="1"/>
0268	</ResponseHeader>
0269	<BatchItem>
0270	<Operation type="Enumeration" value="Get"/>
0271	<ResultStatus type="Enumeration" value="Success"/>
0272	<ResponsePayload>
0273	<ObjectType type="Enumeration" value="SymmetricKey"/>
0274	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0275	<SymmetricKey>
0276	<KeyBlock>
0277	<KeyFormatType type="Enumeration" value="Raw"/>
0278	<KeyValue>
0279	<KeyMaterial type="ByteString"
	value="cc9e3b20f5c4fc4d1298f68d0b7de65b"/>
0280	</KeyValue>
0281	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0282	<CryptographicLength type="Integer" value="128"/>
0283	</KeyBlock>
0284	</SymmetricKey>
0285	</ResponsePayload>
0286	</BatchItem>
0287	</ResponseMessage>
	# TIME 7
	# [Client-B]
0288	<RequestMessage>
0289	<RequestHeader>
0290	<ProtocolVersion>
0291	<ProtocolVersionMajor type="Integer" value="1"/>
0292	<ProtocolVersionMinor type="Integer" value="2"/>
0293	</ProtocolVersion>
0294	<AsynchronousIndicator type="Boolean" value="true"/>
0295	<BatchCount type="Integer" value="1"/>
0296	</RequestHeader>
0297	<BatchItem>

0298	<Operation type="Enumeration" value="Locate"/>
0299	<RequestPayload>
0300	<Attribute>
0301	<AttributeName type="TextString" value="Object Type"/>
0302	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0303	</Attribute>
0304	<Attribute>
0305	<AttributeName type="TextString" value="Name"/>
0306	<AttributeValue>
0307	<NameValue type="TextString" value="TC-32-12-key1"/>
0308	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0309	</AttributeValue>
0310	</Attribute>
0311	</RequestPayload>
0312	</BatchItem>
0313	</RequestMessage>
0314	<ResponseMessage>
0315	<ResponseHeader>
0316	<ProtocolVersion>
0317	<ProtocolVersionMajor type="Integer" value="1"/>
0318	<ProtocolVersionMinor type="Integer" value="2"/>
0319	</ProtocolVersion>
0320	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0321	<BatchCount type="Integer" value="1"/>
0322	</ResponseHeader>
0323	<BatchItem>
0324	<Operation type="Enumeration" value="Locate"/>
0325	<ResultStatus type="Enumeration" value="OperationPending"/>
0326	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0327	</BatchItem>
0328	</ResponseMessage>
	# TIME 8
	# [Client-B]
0329	<RequestMessage>
0330	<RequestHeader>
0331	<ProtocolVersion>
0332	<ProtocolVersionMajor type="Integer" value="1"/>
0333	<ProtocolVersionMinor type="Integer" value="2"/>
0334	</ProtocolVersion>
0335	<BatchCount type="Integer" value="1"/>
0336	</RequestHeader>
0337	<BatchItem>
0338	<Operation type="Enumeration" value="Cancel"/>
0339	<RequestPayload>
0340	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0341	</RequestPayload>
0342	</BatchItem>
0343	</RequestMessage>
0344	<ResponseMessage>
0345	<ResponseHeader>
0346	<ProtocolVersion>
0347	<ProtocolVersionMajor type="Integer" value="1"/>
0348	<ProtocolVersionMinor type="Integer" value="2"/>

0349	</ProtocolVersion>
0350	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0351	<BatchCount type="Integer" value="1"/>
0352	</ResponseHeader>
0353	<BatchItem>
0354	<Operation type="Enumeration" value="Cancel"/>
0355	<ResultStatus type="Enumeration" value="Success"/>
0356	<ResponsePayload>
0357	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0358	<CancellationResult type="Enumeration" value="Canceled"/>
0359	</ResponsePayload>
0360	</BatchItem>
0361	</ResponseMessage>
	# TIME 9
	# [Client-A]
0362	<RequestMessage>
0363	<RequestHeader>
0364	<ProtocolVersion>
0365	<ProtocolVersionMajor type="Integer" value="1"/>
0366	<ProtocolVersionMinor type="Integer" value="2"/>
0367	</ProtocolVersion>
0368	<BatchCount type="Integer" value="1"/>
0369	</RequestHeader>
0370	<BatchItem>
0371	<Operation type="Enumeration" value="Destroy"/>
0372	<RequestPayload>
0373	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0374	</RequestPayload>
0375	</BatchItem>
0376	</RequestMessage>
0377	<ResponseMessage>
0378	<ResponseHeader>
0379	<ProtocolVersion>
0380	<ProtocolVersionMajor type="Integer" value="1"/>
0381	<ProtocolVersionMinor type="Integer" value="2"/>
0382	</ProtocolVersion>
0383	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0384	<BatchCount type="Integer" value="1"/>
0385	</ResponseHeader>
0386	<BatchItem>
0387	<Operation type="Enumeration" value="Destroy"/>
0388	<ResultStatus type="Enumeration" value="Success"/>
0389	<ResponsePayload>
0390	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0391	</ResponsePayload>
0392	</BatchItem>
0393	</ResponseMessage>

785

786 2.3.7 TC-41-12 - Revoke Scenario

787 This test case tests the revocation aspect of the key life cycle support in KMIP. A key is created
788 and a Get Attribute for the State-attribute reveals that the key is in Pre-active state. The

789 Activation Date is then set, which changes the state to Active. The key is then revoked with a
790 revocation reason of Compromised and the state subsequently changed to Compromised, but
791 this does not stop a client from being able to add, modify and delete attributes or even get the
792 key. To clean up, the created key is finally destroyed.

	# TIME 0
	# [Client-A]
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Length"/>
0022	<AttributeValue type="Integer" value="128"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Name"/>
0026	<AttributeValue type="TextString" value="TC-41-12-key1"/>
0027	<NameType type="Enumeration"
0028	value="UninterpretedTextString"/>
0029	</Attribute>
0030	<Attribute>
0031	<AttributeName type="TextString" value="Cryptographic
0032	Usage Mask"/>
0033	<AttributeValue type="Integer" value="Encrypt"/>
0034	</Attribute>
0035	</TemplateAttribute>
0036	</RequestPayload>
0037	</BatchItem>
0038	</RequestMessage>
0039	<ResponseMessage>
0040	<ResponseHeader>
0041	<ProtocolVersion>
0042	<ProtocolVersionMajor type="Integer" value="1"/>
0043	<ProtocolVersionMinor type="Integer" value="2"/>
0044	</ProtocolVersion>
0045	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
	<BatchCount type="Integer" value="1"/>
	</ResponseHeader>

0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
	# TIME 1
	# [Client-A]
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="2"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="GetAttributes"/>
0065	<RequestPayload>
0066	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0067	<AttributeName type="TextString" value="State"/>
0068	</RequestPayload>
0069	</BatchItem>
0070	</RequestMessage>
0071	<ResponseMessage>
0072	<ResponseHeader>
0073	<ProtocolVersion>
0074	<ProtocolVersionMajor type="Integer" value="1"/>
0075	<ProtocolVersionMinor type="Integer" value="2"/>
0076	</ProtocolVersion>
0077	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0078	<BatchCount type="Integer" value="1"/>
0079	</ResponseHeader>
0080	<BatchItem>
0081	<Operation type="Enumeration" value="GetAttributes"/>
0082	<ResultStatus type="Enumeration" value="Success"/>
0083	<ResponsePayload>
0084	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0085	<Attribute>
0086	<AttributeName type="TextString" value="State"/>
0087	<AttributeValue type="Enumeration" value="PreActive"/>
0088	</Attribute>
0089	</ResponsePayload>
0090	</BatchItem>
0091	</ResponseMessage>
	# TIME 2
	# [Client-A]
0092	<RequestMessage>
0093	<RequestHeader>
0094	<ProtocolVersion>

0095	<ProtocolVersionMajor type="Integer" value="1"/>
0096	<ProtocolVersionMinor type="Integer" value="2"/>
0097	</ProtocolVersion>
0098	<BatchCount type="Integer" value="1"/>
0099	</RequestHeader>
0100	<BatchItem>
0101	<Operation type="Enumeration" value="Activate"/>
0102	<RequestPayload>
0103	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0104	</RequestPayload>
0105	</BatchItem>
0106	</RequestMessage>
0107	<ResponseMessage>
0108	<ResponseHeader>
0109	<ProtocolVersion>
0110	<ProtocolVersionMajor type="Integer" value="1"/>
0111	<ProtocolVersionMinor type="Integer" value="2"/>
0112	</ProtocolVersion>
0113	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0114	<BatchCount type="Integer" value="1"/>
0115	</ResponseHeader>
0116	<BatchItem>
0117	<Operation type="Enumeration" value="Activate"/>
0118	<ResultStatus type="Enumeration" value="Success"/>
0119	<ResponsePayload>
0120	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0121	</ResponsePayload>
0122	</BatchItem>
0123	</ResponseMessage>
	# TIME 3
	# [Client-A]
0124	<RequestMessage>
0125	<RequestHeader>
0126	<ProtocolVersion>
0127	<ProtocolVersionMajor type="Integer" value="1"/>
0128	<ProtocolVersionMinor type="Integer" value="2"/>
0129	</ProtocolVersion>
0130	<BatchCount type="Integer" value="1"/>
0131	</RequestHeader>
0132	<BatchItem>
0133	<Operation type="Enumeration" value="GetAttributes"/>
0134	<RequestPayload>
0135	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0136	<AttributeName type="TextString" value="State"/>
0137	</RequestPayload>
0138	</BatchItem>
0139	</RequestMessage>
0140	<ResponseMessage>
0141	<ResponseHeader>
0142	<ProtocolVersion>
0143	<ProtocolVersionMajor type="Integer" value="1"/>
0144	<ProtocolVersionMinor type="Integer" value="2"/>
0145	</ProtocolVersion>

0146	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0147	<BatchCount type="Integer" value="1"/>
0148	</ResponseHeader>
0149	<BatchItem>
0150	<Operation type="Enumeration" value="GetAttributes"/>
0151	<ResultStatus type="Enumeration" value="Success"/>
0152	<ResponsePayload>
0153	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0154	<Attribute>
0155	<AttributeName type="TextString" value="State"/>
0156	<AttributeValue type="Enumeration" value="Active"/>
0157	</Attribute>
0158	</ResponsePayload>
0159	</BatchItem>
0160	</ResponseMessage>
	# TIME 4
	# [Client-B]
0161	<RequestMessage>
0162	<RequestHeader>
0163	<ProtocolVersion>
0164	<ProtocolVersionMajor type="Integer" value="1"/>
0165	<ProtocolVersionMinor type="Integer" value="2"/>
0166	</ProtocolVersion>
0167	<BatchCount type="Integer" value="1"/>
0168	</RequestHeader>
0169	<BatchItem>
0170	<Operation type="Enumeration" value="Locate"/>
0171	<RequestPayload>
0172	<Attribute>
0173	<AttributeName type="TextString" value="Object Type"/>
0174	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0175	</Attribute>
0176	<Attribute>
0177	<AttributeName type="TextString" value="Name"/>
0178	<AttributeValue>
0179	<NameValue type="TextString" value="TC-41-12-key1"/>
0180	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0181	</AttributeValue>
0182	</Attribute>
0183	</RequestPayload>
0184	</BatchItem>
0185	</RequestMessage>
0186	<ResponseMessage>
0187	<ResponseHeader>
0188	<ProtocolVersion>
0189	<ProtocolVersionMajor type="Integer" value="1"/>
0190	<ProtocolVersionMinor type="Integer" value="2"/>
0191	</ProtocolVersion>
0192	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0193	<BatchCount type="Integer" value="1"/>
0194	</ResponseHeader>
0195	<BatchItem>
0196	<Operation type="Enumeration" value="Locate"/>
0197	<ResultStatus type="Enumeration" value="Success"/>
0198	<ResponsePayload>

0199	<UniqueIdentifier type="TextString"
0200	value="\$UNIQUE_IDENTIFIER_0"/>
0201	</ResponsePayload>
0202	</BatchItem>
0203	</ResponseMessage>
# TIME 5	
# [Client-B]	
0203	<RequestMessage>
0204	<RequestHeader>
0205	<ProtocolVersion>
0206	<ProtocolVersionMajor type="Integer" value="1"/>
0207	<ProtocolVersionMinor type="Integer" value="2"/>
0208	</ProtocolVersion>
0209	<BatchCount type="Integer" value="1"/>
0210	</RequestHeader>
0211	<BatchItem>
0212	<Operation type="Enumeration" value="Get"/>
0213	<RequestPayload>
0214	<UniqueIdentifier type="TextString"
0215	value="\$UNIQUE_IDENTIFIER_0"/>
0216	</RequestPayload>
0217	</BatchItem>
0218	</RequestMessage>
0219	<ResponseMessage>
0220	<ResponseHeader>
0221	<ProtocolVersion>
0222	<ProtocolVersionMajor type="Integer" value="1"/>
0223	<ProtocolVersionMinor type="Integer" value="2"/>
0224	</ProtocolVersion>
0225	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0226	<BatchCount type="Integer" value="1"/>
0227	</ResponseHeader>
0228	<BatchItem>
0229	<Operation type="Enumeration" value="Get"/>
0230	<ResultStatus type="Enumeration" value="Success"/>
0231	<ResponsePayload>
0232	<ObjectType type="Enumeration" value="SymmetricKey"/>
0233	<UniqueIdentifier type="TextString"
0234	value="\$UNIQUE_IDENTIFIER_0"/>
0235	<SymmetricKey>
0236	<KeyBlock>
0237	<KeyFormatType type="Enumeration" value="Raw"/>
0238	<KeyValue>
0239	<KeyMaterial type="ByteString"
0240	value="9c7d7c4fd2076f1909a6ba4342cab1de"/>
0241	</KeyValue>
0242	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0243	<CryptographicLength type="Integer" value="128"/>
0244	</KeyBlock>
0245	</SymmetricKey>
0246	</ResponsePayload>
0247	</BatchItem>
0248	</ResponseMessage>
# TIME 6	
# [Client-B]	
0249	<RequestMessage>

0247	<RequestHeader>
0248	<ProtocolVersion>
0249	<ProtocolVersionMajor type="Integer" value="1"/>
0250	<ProtocolVersionMinor type="Integer" value="2"/>
0251	</ProtocolVersion>
0252	<BatchCount type="Integer" value="1"/>
0253	</RequestHeader>
0254	<BatchItem>
0255	<Operation type="Enumeration" value="Revoke"/>
0256	<RequestPayload>
0257	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0258	<RevocationReason>
0259	<RevocationReasonCode type="Enumeration"
	value="KeyCompromise"/>
0260	</RevocationReason>
0261	<CompromiseOccurrenceDate type="DateTime" value="1970-01-
	01T00:00:06+00:00"/>
0262	</RequestPayload>
0263	</BatchItem>
0264	</RequestMessage>
0265	<ResponseMessage>
0266	<ResponseHeader>
0267	<ProtocolVersion>
0268	<ProtocolVersionMajor type="Integer" value="1"/>
0269	<ProtocolVersionMinor type="Integer" value="2"/>
0270	</ProtocolVersion>
0271	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0272	<BatchCount type="Integer" value="1"/>
0273	</ResponseHeader>
0274	<BatchItem>
0275	<Operation type="Enumeration" value="Revoke"/>
0276	<ResultStatus type="Enumeration" value="Success"/>
0277	<ResponsePayload>
0278	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0279	</ResponsePayload>
0280	</BatchItem>
0281	</ResponseMessage>
	# TIME 7
	# [Client-B]
0282	<RequestMessage>
0283	<RequestHeader>
0284	<ProtocolVersion>
0285	<ProtocolVersionMajor type="Integer" value="1"/>
0286	<ProtocolVersionMinor type="Integer" value="2"/>
0287	</ProtocolVersion>
0288	<BatchCount type="Integer" value="1"/>
0289	</RequestHeader>
0290	<BatchItem>
0291	<Operation type="Enumeration" value="GetAttributes"/>
0292	<RequestPayload>
0293	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0294	<AttributeName type="TextString" value="State"/>
0295	</RequestPayload>
0296	</BatchItem>

0297	</RequestMessage>
0298	<ResponseMessage>
0299	<ResponseHeader>
0300	<ProtocolVersion>
0301	<ProtocolVersionMajor type="Integer" value="1"/>
0302	<ProtocolVersionMinor type="Integer" value="2"/>
0303	</ProtocolVersion>
0304	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0305	<BatchCount type="Integer" value="1"/>
0306	</ResponseHeader>
0307	<BatchItem>
0308	<Operation type="Enumeration" value="GetAttributes"/>
0309	<ResultStatus type="Enumeration" value="Success"/>
0310	<ResponsePayload>
0311	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0312	<Attribute>
0313	<AttributeName type="TextString" value="State"/>
0314	<AttributeValue type="Enumeration" value="Compromised"/>
0315	</Attribute>
0316	</ResponsePayload>
0317	</BatchItem>
0318	</ResponseMessage>
# TIME 8 # [Client-A]	
0319	<RequestMessage>
0320	<RequestHeader>
0321	<ProtocolVersion>
0322	<ProtocolVersionMajor type="Integer" value="1"/>
0323	<ProtocolVersionMinor type="Integer" value="2"/>
0324	</ProtocolVersion>
0325	<BatchCount type="Integer" value="1"/>
0326	</RequestHeader>
0327	<BatchItem>
0328	<Operation type="Enumeration" value="GetAttributeList"/>
0329	<RequestPayload>
0330	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0331	</RequestPayload>
0332	</BatchItem>
0333	</RequestMessage>
0334	<ResponseMessage>
0335	<ResponseHeader>
0336	<ProtocolVersion>
0337	<ProtocolVersionMajor type="Integer" value="1"/>
0338	<ProtocolVersionMinor type="Integer" value="2"/>
0339	</ProtocolVersion>
0340	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0341	<BatchCount type="Integer" value="1"/>
0342	</ResponseHeader>
0343	<BatchItem>
0344	<Operation type="Enumeration" value="GetAttributeList"/>
0345	<ResultStatus type="Enumeration" value="Success"/>
0346	<ResponsePayload>
0347	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0348	<AttributeName type="TextString" value="Unique Identifier"/>
0349	<AttributeName type="TextString" value="Object Type"/>
0350	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0351	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0352	<AttributeName type="TextString" value="Activation Date"/>
0353	<AttributeName type="TextString" value="Compromise Date"/>
0354	<AttributeName type="TextString" value="Compromise Occurrence
	Date"/>
0355	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0356	<AttributeName type="TextString" value="Digest"/>
0357	<AttributeName type="TextString" value="Fresh"/>
0358	<AttributeName type="TextString" value="Initial Date"/>
0359	<AttributeName type="TextString" value="Last Change Date"/>
0360	<AttributeName type="TextString" value="Lease Time"/>
0361	<AttributeName type="TextString" value="Name"/>
0362	<AttributeName type="TextString" value="Original Creation
	Date"/>
0363	<AttributeName type="TextString" value="Revocation Reason"/>
0364	<AttributeName type="TextString" value="State"/>
0365	</ResponsePayload>
0366	</BatchItem>
0367	</ResponseMessage>
	# TIME 9
	# [Client-A]
0368	<RequestMessage>
0369	<RequestHeader>
0370	<ProtocolVersion>
0371	<ProtocolVersionMajor type="Integer" value="1"/>
0372	<ProtocolVersionMinor type="Integer" value="2"/>
0373	</ProtocolVersion>
0374	<BatchCount type="Integer" value="1"/>
0375	</RequestHeader>
0376	<BatchItem>
0377	<Operation type="Enumeration" value="GetAttributes"/>
0378	<RequestPayload>
0379	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0380	<AttributeName type="TextString" value="State"/>
0381	</RequestPayload>
0382	</BatchItem>
0383	</RequestMessage>
0384	<ResponseMessage>
0385	<ResponseHeader>
0386	<ProtocolVersion>
0387	<ProtocolVersionMajor type="Integer" value="1"/>
0388	<ProtocolVersionMinor type="Integer" value="2"/>
0389	</ProtocolVersion>
0390	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0391	<BatchCount type="Integer" value="1"/>
0392	</ResponseHeader>
0393	<BatchItem>
0394	<Operation type="Enumeration" value="GetAttributes"/>
0395	<ResultStatus type="Enumeration" value="Success"/>
0396	<ResponsePayload>

0397	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0398	<Attribute>
0399	<AttributeName type="TextString" value="State"/>
0400	<AttributeValue type="Enumeration" value="Compromised"/>
0401	</Attribute>
0402	</ResponsePayload>
0403	</BatchItem>
0404	</ResponseMessage>
	# TIME 10
	# [Client-A]
0405	<RequestMessage>
0406	<RequestHeader>
0407	<ProtocolVersion>
0408	<ProtocolVersionMajor type="Integer" value="1"/>
0409	<ProtocolVersionMinor type="Integer" value="2"/>
0410	</ProtocolVersion>
0411	<BatchCount type="Integer" value="2"/>
0412	</RequestHeader>
0413	<BatchItem>
0414	<Operation type="Enumeration" value="AddAttribute"/>
0415	<UniqueBatchItemID type="ByteString" value="23a177faa569463c"/>
0416	<RequestPayload>
0417	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0418	<Attribute>
0419	<AttributeName type="TextString" value="x-attribute1"/>
0420	<AttributeValue type="TextString" value="Value1"/>
0421	</Attribute>
0422	</RequestPayload>
0423	</BatchItem>
0424	<BatchItem>
0425	<Operation type="Enumeration" value="AddAttribute"/>
0426	<UniqueBatchItemID type="ByteString" value="9b898dc0577f8080"/>
0427	<RequestPayload>
0428	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0429	<Attribute>
0430	<AttributeName type="TextString" value="x-attribute2"/>
0431	<AttributeValue type="TextString" value="Value2"/>
0432	</Attribute>
0433	</RequestPayload>
0434	</BatchItem>
0435	</RequestMessage>
	# [Client-A]
0436	<ResponseMessage>
0437	<ResponseHeader>
0438	<ProtocolVersion>
0439	<ProtocolVersionMajor type="Integer" value="1"/>
0440	<ProtocolVersionMinor type="Integer" value="2"/>
0441	</ProtocolVersion>
0442	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0443	<BatchCount type="Integer" value="2"/>
0444	</ResponseHeader>
0445	<BatchItem>
0446	<Operation type="Enumeration" value="AddAttribute"/>
0447	<UniqueBatchItemID type="ByteString" value="23a177faa569463c"/>

0448	<ResultStatus type="Enumeration" value="Success"/>
0449	<ResponsePayload>
0450	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0451	<Attribute>
0452	<AttributeName type="TextString" value="x-attribute1"/>
0453	<AttributeValue type="TextString" value="Value1"/>
0454	</Attribute>
0455	</ResponsePayload>
0456	</BatchItem>
0457	<BatchItem>
0458	<Operation type="Enumeration" value="AddAttribute"/>
0459	<UniqueBatchItemID type="ByteString" value="9b898dc0577f8080"/>
0460	<ResultStatus type="Enumeration" value="Success"/>
0461	<ResponsePayload>
0462	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0463	<Attribute>
0464	<AttributeName type="TextString" value="x-attribute2"/>
0465	<AttributeValue type="TextString" value="Value2"/>
0466	</Attribute>
0467	</ResponsePayload>
0468	</BatchItem>
0469	</ResponseMessage>
	# TIME 11
	# [Client-A]
0470	<RequestMessage>
0471	<RequestHeader>
0472	<ProtocolVersion>
0473	<ProtocolVersionMajor type="Integer" value="1"/>
0474	<ProtocolVersionMinor type="Integer" value="2"/>
0475	</ProtocolVersion>
0476	<BatchCount type="Integer" value="2"/>
0477	</RequestHeader>
0478	<BatchItem>
0479	<Operation type="Enumeration" value="ModifyAttribute"/>
0480	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0481	<RequestPayload>
0482	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0483	<Attribute>
0484	<AttributeName type="TextString" value="x-attribute1"/>
0485	<AttributeValue type="TextString" value="ModifiedValue1"/>
0486	</Attribute>
0487	</RequestPayload>
0488	</BatchItem>
0489	<BatchItem>
0490	<Operation type="Enumeration" value="ModifyAttribute"/>
0491	<UniqueBatchItemID type="ByteString" value="33f55c8d7e6cafbf"/>
0492	<RequestPayload>
0493	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0494	<Attribute>
0495	<AttributeName type="TextString" value="x-attribute2"/>
0496	<AttributeValue type="TextString" value="ModifiedValue2"/>
0497	</Attribute>
0498	</RequestPayload>

0499	</BatchItem>
0500	</RequestMessage>
0501	<ResponseMessage>
0502	<ResponseHeader>
0503	<ProtocolVersion>
0504	<ProtocolVersionMajor type="Integer" value="1"/>
0505	<ProtocolVersionMinor type="Integer" value="2"/>
0506	</ProtocolVersion>
0507	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0508	<BatchCount type="Integer" value="2"/>
0509	</ResponseHeader>
0510	<BatchItem>
0511	<Operation type="Enumeration" value="ModifyAttribute"/>
0512	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0513	<ResultStatus type="Enumeration" value="Success"/>
0514	<ResponsePayload>
0515	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0516	<Attribute>
0517	<AttributeName type="TextString" value="x-attribute1"/>
0518	<AttributeValue type="TextString" value="ModifiedValue1"/>
0519	</Attribute>
0520	</ResponsePayload>
0521	</BatchItem>
0522	<BatchItem>
0523	<Operation type="Enumeration" value="ModifyAttribute"/>
0524	<UniqueBatchItemID type="ByteString" value="33f55c8d7e6cafbf"/>
0525	<ResultStatus type="Enumeration" value="Success"/>
0526	<ResponsePayload>
0527	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0528	<Attribute>
0529	<AttributeName type="TextString" value="x-attribute2"/>
0530	<AttributeValue type="TextString" value="ModifiedValue2"/>
0531	</Attribute>
0532	</ResponsePayload>
0533	</BatchItem>
0534	</ResponseMessage>
	# TIME 12
	# [Client-A]
0535	<RequestMessage>
0536	<RequestHeader>
0537	<ProtocolVersion>
0538	<ProtocolVersionMajor type="Integer" value="1"/>
0539	<ProtocolVersionMinor type="Integer" value="2"/>
0540	</ProtocolVersion>
0541	<BatchCount type="Integer" value="2"/>
0542	</RequestHeader>
0543	<BatchItem>
0544	<Operation type="Enumeration" value="DeleteAttribute"/>
0545	<UniqueBatchItemID type="ByteString" value="a3eb249b495e8ad2"/>
0546	<RequestPayload>
0547	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0548	<AttributeName type="TextString" value="x-attribute1"/>
0549	</RequestPayload>
0550	</BatchItem>

0551	<BatchItem>
0552	<Operation type="Enumeration" value="DeleteAttribute"/>
0553	<UniqueBatchItemID type="ByteString" value="c1fe7b3b4c977730"/>
0554	<RequestPayload>
0555	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0556	<AttributeName type="TextString" value="x-attribute2"/>
0557	</RequestPayload>
0558	</BatchItem>
0559	</RequestMessage>
0560	<ResponseMessage>
0561	<ResponseHeader>
0562	<ProtocolVersion>
0563	<ProtocolVersionMajor type="Integer" value="1"/>
0564	<ProtocolVersionMinor type="Integer" value="2"/>
0565	</ProtocolVersion>
0566	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0567	<BatchCount type="Integer" value="2"/>
0568	</ResponseHeader>
0569	<BatchItem>
0570	<Operation type="Enumeration" value="DeleteAttribute"/>
0571	<UniqueBatchItemID type="ByteString" value="a3eb249b495e8ad2"/>
0572	<ResultStatus type="Enumeration" value="Success"/>
0573	<ResponsePayload>
0574	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0575	<Attribute>
0576	<AttributeName type="TextString" value="x-attribute1"/>
0577	<AttributeValue type="TextString" value="ModifiedValue1"/>
0578	</Attribute>
0579	</ResponsePayload>
0580	</BatchItem>
0581	<BatchItem>
0582	<Operation type="Enumeration" value="DeleteAttribute"/>
0583	<UniqueBatchItemID type="ByteString" value="c1fe7b3b4c977730"/>
0584	<ResultStatus type="Enumeration" value="Success"/>
0585	<ResponsePayload>
0586	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0587	<Attribute>
0588	<AttributeName type="TextString" value="x-attribute2"/>
0589	<AttributeValue type="TextString" value="ModifiedValue2"/>
0590	</Attribute>
0591	</ResponsePayload>
0592	</BatchItem>
0593	</ResponseMessage>
	# TIME 13
	# [Client-A]
0594	<RequestMessage>
0595	<RequestHeader>
0596	<ProtocolVersion>
0597	<ProtocolVersionMajor type="Integer" value="1"/>
0598	<ProtocolVersionMinor type="Integer" value="2"/>
0599	</ProtocolVersion>
0600	<BatchCount type="Integer" value="1"/>
0601	</RequestHeader>
0602	<BatchItem>

0603	<Operation type="Enumeration" value="Get"/>
0604	<RequestPayload>
0605	<UniqueIdentifier type="TextString"
0606	value="\$UNIQUE_IDENTIFIER_0"/>
0607	</RequestPayload>
0608	</BatchItem>
0609	</RequestMessage>
0610	<ResponseMessage>
0611	<ResponseHeader>
0612	<ProtocolVersion>
0613	<ProtocolVersionMajor type="Integer" value="1"/>
0614	<ProtocolVersionMinor type="Integer" value="2"/>
0615	</ProtocolVersion>
0616	<Timestamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0617	<BatchCount type="Integer" value="1"/>
0618	</ResponseHeader>
0619	<BatchItem>
0620	<Operation type="Enumeration" value="Get"/>
0621	<ResultStatus type="Enumeration" value="Success"/>
0622	<ResponsePayload>
0623	<ObjectType type="Enumeration" value="SymmetricKey"/>
0624	<UniqueIdentifier type="TextString"
0625	value="\$UNIQUE_IDENTIFIER_0"/>
0626	<SymmetricKey>
0627	<KeyBlock>
0628	<KeyFormatType type="Enumeration" value="Raw"/>
0629	<KeyValue>
0630	<KeyMaterial type="ByteString"
0631	value="9c7d7c4fd2076f1909a6ba4342cab1de"/>
0632	</KeyValue>
0633	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0634	<CryptographicLength type="Integer" value="128"/>
0635	</CryptographicLength>
0636	</KeyBlock>
0637	</SymmetricKey>
0638	</ResponsePayload>
0639	</BatchItem>
0640	</ResponseMessage>
0641	# TIME 14
0642	# [Client-A]
0643	<RequestMessage>
0644	<RequestHeader>
0645	<ProtocolVersion>
0646	<ProtocolVersionMajor type="Integer" value="1"/>
0647	<ProtocolVersionMinor type="Integer" value="2"/>
0648	</ProtocolVersion>
0649	<BatchCount type="Integer" value="1"/>
0650	</RequestHeader>
0651	<BatchItem>
0652	<Operation type="Enumeration" value="Destroy"/>
0653	<RequestPayload>
0654	<UniqueIdentifier type="TextString"
0655	value="\$UNIQUE_IDENTIFIER_0"/>
0656	</RequestPayload>
0657	</BatchItem>
0658	</RequestMessage>
0659	<ResponseMessage>

```

0653 <ResponseHeader>
0654   <ProtocolVersion>
0655     <ProtocolVersionMajor type="Integer" value="1"/>
0656     <ProtocolVersionMinor type="Integer" value="2"/>
0657   </ProtocolVersion>
0658   <TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0659   <BatchCount type="Integer" value="1"/>
0660 </ResponseHeader>
0661 <BatchItem>
0662   <Operation type="Enumeration" value="Destroy"/>
0663   <ResultStatus type="Enumeration" value="Success"/>
0664   <ResponsePayload>
0665     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0666   </ResponsePayload>
0667 </BatchItem>
0668 </ResponseMessage>

```

793

794 2.3.8 TC-51-12 - Get Usage Allocation Scenario

795 This test case tests the usage management functionality of KMIP. A key is created and the
796 Activation Date and Protect Stop Date attributes are set in such a way as to allow the Get Usage
797 Allocation operation to be performed. The value of the Usage Limits attribute is set to 1000
798 bytes, and two subsequent requests for 500 bytes succeed (one of them also verifying the
799 amount that can be received using the Check operation), while a third fails since the usage
800 allocation has been used up. The key is finally revoked and destroyed. This test case shows the
801 use of multiple clients (Client-A, Client-B and Client-C).

```

# TIME 0
# [Client-A]
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="2"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="Create"/>
0011     <RequestPayload>
0012       <ObjectType type="Enumeration" value="SymmetricKey"/>
0013       <TemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0016           <AttributeValue type="Enumeration" value="AES"/>
0017         </Attribute>
0018         <Attribute>
0019           <AttributeName type="TextString" value="Cryptographic
Length"/>
0020           <AttributeValue type="Integer" value="128"/>
0021         </Attribute>

```

0022	<Attribute>
0023	<AttributeName type="TextString" value="Name"/>
0024	<AttributeValue>
0025	<NameValue type="TextString" value="TC-51-12-key1"/>
0026	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0027	</AttributeValue>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0031	<AttributeValue type="Integer" value="Encrypt"/>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="2"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
	# TIME 1
	# [Client-A]
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="2"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="2"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="AddAttribute"/>
0065	<UniqueBatchItemID type="ByteString" value="369f6802ee57532b"/>
0066	<RequestPayload>
0067	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0068	<Attribute>
0069	<AttributeName type="TextString" value="Activation Date"/>
0070	<AttributeValue type="DateTime" value="1970-01-
	01T00:00:02+00:00"/>
0071	</Attribute>

0072	</RequestPayload>
0073	</BatchItem>
0074	<BatchItem>
0075	<Operation type="Enumeration" value="AddAttribute"/>
0076	<UniqueBatchItemID type="ByteString" value="b7ca806e52825bf4"/>
0077	<RequestPayload>
0078	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0079	<Attribute>
0080	<AttributeName type="TextString" value="Protect Stop Date"/>
0081	<AttributeValue type="DateTime" value="\$NOW+600"/>
0082	</Attribute>
0083	</RequestPayload>
0084	</BatchItem>
0085	</RequestMessage>
0086	<ResponseMessage>
0087	<ResponseHeader>
0088	<ProtocolVersion>
0089	<ProtocolVersionMajor type="Integer" value="1"/>
0090	<ProtocolVersionMinor type="Integer" value="2"/>
0091	</ProtocolVersion>
0092	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0093	<BatchCount type="Integer" value="2"/>
0094	</ResponseHeader>
0095	<BatchItem>
0096	<Operation type="Enumeration" value="AddAttribute"/>
0097	<UniqueBatchItemID type="ByteString" value="369f6802ee57532b"/>
0098	<ResultStatus type="Enumeration" value="Success"/>
0099	<ResponsePayload>
0100	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0101	<Attribute>
0102	<AttributeName type="TextString" value="Activation Date"/>
0103	<AttributeValue type="DateTime" value="1970-01-
	01T00:00:02+00:00"/>
0104	</Attribute>
0105	</ResponsePayload>
0106	</BatchItem>
0107	<BatchItem>
0108	<Operation type="Enumeration" value="AddAttribute"/>
0109	<UniqueBatchItemID type="ByteString" value="b7ca806e52825bf4"/>
0110	<ResultStatus type="Enumeration" value="Success"/>
0111	<ResponsePayload>
0112	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0113	<Attribute>
0114	<AttributeName type="TextString" value="Protect Stop Date"/>
0115	<AttributeValue type="DateTime" value="\$NOW+600"/>
0116	</Attribute>
0117	</ResponsePayload>
0118	</BatchItem>
0119	</ResponseMessage>
	# TIME 2
	# [Client-A]
0120	<RequestMessage>
0121	<RequestHeader>
0122	<ProtocolVersion>

0123	<ProtocolVersionMajor type="Integer" value="1"/>
0124	<ProtocolVersionMinor type="Integer" value="2"/>
0125	</ProtocolVersion>
0126	<BatchCount type="Integer" value="1"/>
0127	</RequestHeader>
0128	<BatchItem>
0129	<Operation type="Enumeration" value="AddAttribute"/>
0130	<RequestPayload>
0131	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0132	<Attribute>
0133	<AttributeName type="TextString" value="Usage Limits"/>
0134	<AttributeValue>
0135	<UsageLimitsTotal type="LongInteger" value="1000"/>
0136	<UsageLimitsUnit type="Enumeration" value="Byte"/>
0137	</AttributeValue>
0138	</Attribute>
0139	</RequestPayload>
0140	</BatchItem>
0141	</RequestMessage>
0142	<ResponseMessage>
0143	<ResponseHeader>
0144	<ProtocolVersion>
0145	<ProtocolVersionMajor type="Integer" value="1"/>
0146	<ProtocolVersionMinor type="Integer" value="2"/>
0147	</ProtocolVersion>
0148	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0149	<BatchCount type="Integer" value="1"/>
0150	</ResponseHeader>
0151	<BatchItem>
0152	<Operation type="Enumeration" value="AddAttribute"/>
0153	<ResultStatus type="Enumeration" value="Success"/>
0154	<ResponsePayload>
0155	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0156	<Attribute>
0157	<AttributeName type="TextString" value="Usage Limits"/>
0158	<AttributeValue>
0159	<UsageLimitsTotal type="LongInteger" value="1000"/>
0160	<UsageLimitsCount type="LongInteger" value="1000"/>
0161	<UsageLimitsUnit type="Enumeration" value="Byte"/>
0162	</AttributeValue>
0163	</Attribute>
0164	</ResponsePayload>
0165	</BatchItem>
0166	</ResponseMessage>
	# TIME 3
	# [Client-B]
0167	<RequestMessage>
0168	<RequestHeader>
0169	<ProtocolVersion>
0170	<ProtocolVersionMajor type="Integer" value="1"/>
0171	<ProtocolVersionMinor type="Integer" value="2"/>
0172	</ProtocolVersion>
0173	<BatchCount type="Integer" value="1"/>
0174	</RequestHeader>
0175	<BatchItem>

0176	<Operation type="Enumeration" value="Locate"/>
0177	<RequestPayload>
0178	<Attribute>
0179	<AttributeName type="TextString" value="Object Type"/>
0180	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0181	</Attribute>
0182	<Attribute>
0183	<AttributeName type="TextString" value="Name"/>
0184	<AttributeValue>
0185	<NameValue type="TextString" value="TC-51-12-key1"/>
0186	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0187	</AttributeValue>
0188	</Attribute>
0189	</RequestPayload>
0190	</BatchItem>
0191	</RequestMessage>
0192	<ResponseMessage>
0193	<ResponseHeader>
0194	<ProtocolVersion>
0195	<ProtocolVersionMajor type="Integer" value="1"/>
0196	<ProtocolVersionMinor type="Integer" value="2"/>
0197	</ProtocolVersion>
0198	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0199	<BatchCount type="Integer" value="1"/>
0200	</ResponseHeader>
0201	<BatchItem>
0202	<Operation type="Enumeration" value="Locate"/>
0203	<ResultStatus type="Enumeration" value="Success"/>
0204	<ResponsePayload>
0205	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0206	</ResponsePayload>
0207	</BatchItem>
0208	</ResponseMessage>
0209	# TIME 4
	# [Client-B]
0210	<RequestMessage>
0211	<RequestHeader>
0212	<ProtocolVersion>
0213	<ProtocolVersionMajor type="Integer" value="1"/>
0214	<ProtocolVersionMinor type="Integer" value="2"/>
0215	</ProtocolVersion>
0216	<BatchCount type="Integer" value="1"/>
0217	</RequestHeader>
0218	<BatchItem>
0219	<Operation type="Enumeration" value="Get"/>
0220	<RequestPayload>
	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0221	</RequestPayload>
0222	</BatchItem>
0223	</RequestMessage>
0224	<ResponseMessage>
0225	<ResponseHeader>
0226	<ProtocolVersion>

0227	<ProtocolVersionMajor type="Integer" value="1"/>
0228	<ProtocolVersionMinor type="Integer" value="2"/>
0229	</ProtocolVersion>
0230	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0231	<BatchCount type="Integer" value="1"/>
0232	</ResponseHeader>
0233	<BatchItem>
0234	<Operation type="Enumeration" value="Get"/>
0235	<ResultStatus type="Enumeration" value="Success"/>
0236	<ResponsePayload>
0237	<ObjectType type="Enumeration" value="SymmetricKey"/>
0238	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0239	<SymmetricKey>
0240	<KeyBlock>
0241	<KeyFormatType type="Enumeration" value="Raw"/>
0242	<KeyValue>
0243	<KeyMaterial type="ByteString"
	value="50f31013c771af4448110f695efa9ec7"/>
0244	</KeyValue>
0245	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0246	<CryptographicLength type="Integer" value="128"/>
0247	</KeyBlock>
0248	</SymmetricKey>
0249	</ResponsePayload>
0250	</BatchItem>
0251	</ResponseMessage>
	# TIME 5
	# [Client-B]
0252	<RequestMessage>
0253	<RequestHeader>
0254	<ProtocolVersion>
0255	<ProtocolVersionMajor type="Integer" value="1"/>
0256	<ProtocolVersionMinor type="Integer" value="2"/>
0257	</ProtocolVersion>
0258	<BatchOrderOption type="Boolean" value="true"/>
0259	<BatchCount type="Integer" value="2"/>
0260	</RequestHeader>
0261	<BatchItem>
0262	<Operation type="Enumeration" value="Check"/>
0263	<UniqueBatchItemID type="ByteString" value="d35a294f9425f06e"/>
0264	<RequestPayload>
0265	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0266	<UsageLimitsCount type="LongInteger" value="500"/>
0267	</RequestPayload>
0268	</BatchItem>
0269	<BatchItem>
0270	<Operation type="Enumeration" value="GetUsageAllocation"/>
0271	<UniqueBatchItemID type="ByteString" value="80454d8ce4f738fe"/>
0272	<RequestPayload>
0273	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0274	<UsageLimitsCount type="LongInteger" value="500"/>
0275	</RequestPayload>
0276	</BatchItem>
0277	</RequestMessage>

0278	<ResponseMessage>
0279	<ResponseHeader>
0280	<ProtocolVersion>
0281	<ProtocolVersionMajor type="Integer" value="1"/>
0282	<ProtocolVersionMinor type="Integer" value="2"/>
0283	</ProtocolVersion>
0284	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0285	<BatchCount type="Integer" value="2"/>
0286	</ResponseHeader>
0287	<BatchItem>
0288	<Operation type="Enumeration" value="Check"/>
0289	<UniqueBatchItemID type="ByteString" value="d35a294f9425f06e"/>
0290	<ResultStatus type="Enumeration" value="Success"/>
0291	<ResponsePayload>
0292	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0293	</ResponsePayload>
0294	</BatchItem>
0295	<BatchItem>
0296	<Operation type="Enumeration" value="GetUsageAllocation"/>
0297	<UniqueBatchItemID type="ByteString" value="80454d8ce4f738fe"/>
0298	<ResultStatus type="Enumeration" value="Success"/>
0299	<ResponsePayload>
0300	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0301	</ResponsePayload>
0302	</BatchItem>
0303	</ResponseMessage>
	# TIME 6
	# [Client-A]
0304	<RequestMessage>
0305	<RequestHeader>
0306	<ProtocolVersion>
0307	<ProtocolVersionMajor type="Integer" value="1"/>
0308	<ProtocolVersionMinor type="Integer" value="2"/>
0309	</ProtocolVersion>
0310	<BatchCount type="Integer" value="1"/>
0311	</RequestHeader>
0312	<BatchItem>
0313	<Operation type="Enumeration" value="GetUsageAllocation"/>
0314	<RequestPayload>
0315	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0316	<UsageLimitsCount type="LongInteger" value="500"/>
0317	</RequestPayload>
0318	</BatchItem>
0319	</RequestMessage>
0320	<ResponseMessage>
0321	<ResponseHeader>
0322	<ProtocolVersion>
0323	<ProtocolVersionMajor type="Integer" value="1"/>
0324	<ProtocolVersionMinor type="Integer" value="2"/>
0325	</ProtocolVersion>
0326	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0327	<BatchCount type="Integer" value="1"/>
0328	</ResponseHeader>
0329	<BatchItem>

0330	<Operation type="Enumeration" value="GetUsageAllocation"/>
0331	<ResultStatus type="Enumeration" value="Success"/>
0332	<ResponsePayload>
0333	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0334	</ResponsePayload>
0335	</BatchItem>
0336	</ResponseMessage>
	# TIME 7
	# [Client-C]
0337	<RequestMessage>
0338	<RequestHeader>
0339	<ProtocolVersion>
0340	<ProtocolVersionMajor type="Integer" value="1"/>
0341	<ProtocolVersionMinor type="Integer" value="2"/>
0342	</ProtocolVersion>
0343	<BatchCount type="Integer" value="1"/>
0344	</RequestHeader>
0345	<BatchItem>
0346	<Operation type="Enumeration" value="Locate"/>
0347	<RequestPayload>
0348	<Attribute>
0349	<AttributeName type="TextString" value="Object Type"/>
0350	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0351	</Attribute>
0352	<Attribute>
0353	<AttributeName type="TextString" value="Name"/>
0354	<AttributeValue>
0355	<NameValue type="TextString" value="TC-51-12-key1"/>
0356	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0357	</AttributeValue>
0358	</Attribute>
0359	</RequestPayload>
0360	</BatchItem>
0361	</RequestMessage>
0362	<ResponseMessage>
0363	<ResponseHeader>
0364	<ProtocolVersion>
0365	<ProtocolVersionMajor type="Integer" value="1"/>
0366	<ProtocolVersionMinor type="Integer" value="2"/>
0367	</ProtocolVersion>
0368	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0369	<BatchCount type="Integer" value="1"/>
0370	</ResponseHeader>
0371	<BatchItem>
0372	<Operation type="Enumeration" value="Locate"/>
0373	<ResultStatus type="Enumeration" value="Success"/>
0374	<ResponsePayload>
0375	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0376	</ResponsePayload>
0377	</BatchItem>
0378	</ResponseMessage>
	# TIME 8
	# [Client-C]

0379	<RequestMessage>
0380	<RequestHeader>
0381	<ProtocolVersion>
0382	<ProtocolVersionMajor type="Integer" value="1"/>
0383	<ProtocolVersionMinor type="Integer" value="2"/>
0384	</ProtocolVersion>
0385	<BatchCount type="Integer" value="1"/>
0386	</RequestHeader>
0387	<BatchItem>
0388	<Operation type="Enumeration" value="Get"/>
0389	<RequestPayload>
0390	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0391	</RequestPayload>
0392	</BatchItem>
0393	</RequestMessage>
0394	<ResponseMessage>
0395	<ResponseHeader>
0396	<ProtocolVersion>
0397	<ProtocolVersionMajor type="Integer" value="1"/>
0398	<ProtocolVersionMinor type="Integer" value="2"/>
0399	</ProtocolVersion>
0400	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0401	<BatchCount type="Integer" value="1"/>
0402	</ResponseHeader>
0403	<BatchItem>
0404	<Operation type="Enumeration" value="Get"/>
0405	<ResultStatus type="Enumeration" value="Success"/>
0406	<ResponsePayload>
0407	<ObjectType type="Enumeration" value="SymmetricKey"/>
0408	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0409	<SymmetricKey>
0410	<KeyBlock>
0411	<KeyFormatType type="Enumeration" value="Raw"/>
0412	<KeyValue>
0413	<KeyMaterial type="ByteString"
	value="50f31013c771af4448110f695efa9ec7"/>
0414	</KeyValue>
0415	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0416	<CryptographicLength type="Integer" value="128"/>
0417	</KeyBlock>
0418	</SymmetricKey>
0419	</ResponsePayload>
0420	</BatchItem>
0421	</ResponseMessage>
	# TIME 9
	# [Client-C]
0422	<RequestMessage>
0423	<RequestHeader>
0424	<ProtocolVersion>
0425	<ProtocolVersionMajor type="Integer" value="1"/>
0426	<ProtocolVersionMinor type="Integer" value="2"/>
0427	</ProtocolVersion>
0428	<BatchCount type="Integer" value="1"/>
0429	</RequestHeader>
0430	<BatchItem>

0431	<Operation type="Enumeration" value="GetUsageAllocation"/>
0432	<RequestPayload>
0433	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0434	<UsageLimitsCount type="LongInteger" value="500"/>
0435	</RequestPayload>
0436	</BatchItem>
0437	</RequestMessage>
0438	<ResponseMessage>
0439	<ResponseHeader>
0440	<ProtocolVersion>
0441	<ProtocolVersionMajor type="Integer" value="1"/>
0442	<ProtocolVersionMinor type="Integer" value="2"/>
0443	</ProtocolVersion>
0444	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0445	<BatchCount type="Integer" value="1"/>
0446	</ResponseHeader>
0447	<BatchItem>
0448	<Operation type="Enumeration" value="GetUsageAllocation"/>
0449	<ResultStatus type="Enumeration" value="OperationFailed"/>
0450	<ResultReason type="Enumeration" value="PermissionDenied"/>
0451	<ResultMessage type="TextString" value="Unable to allocate
	requested amount"/>
0452	</BatchItem>
0453	</ResponseMessage>
	# TIME 10
	# [Client-A]
0454	<RequestMessage>
0455	<RequestHeader>
0456	<ProtocolVersion>
0457	<ProtocolVersionMajor type="Integer" value="1"/>
0458	<ProtocolVersionMinor type="Integer" value="2"/>
0459	</ProtocolVersion>
0460	<BatchOrderOption type="Boolean" value="true"/>
0461	<BatchCount type="Integer" value="2"/>
0462	</RequestHeader>
0463	<BatchItem>
0464	<Operation type="Enumeration" value="Revoke"/>
0465	<UniqueBatchItemID type="ByteString" value="79b998c5f29465f4"/>
0466	<RequestPayload>
0467	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0468	<RevocationReason>
0469	<RevocationReasonCode type="Enumeration"
	value="CessationOfOperation"/>
0470	</RevocationReason>
0471	</RequestPayload>
0472	</BatchItem>
0473	<BatchItem>
0474	<Operation type="Enumeration" value="Destroy"/>
0475	<UniqueBatchItemID type="ByteString" value="b0633f0e41187345"/>
0476	<RequestPayload>
0477	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0478	</RequestPayload>
0479	</BatchItem>
0480	</RequestMessage>


```
0481 <ResponseMessage>
0482   <ResponseHeader>
0483     <ProtocolVersion>
0484       <ProtocolVersionMajor type="Integer" value="1"/>
0485       <ProtocolVersionMinor type="Integer" value="2"/>
0486     </ProtocolVersion>
0487     <TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0488     <BatchCount type="Integer" value="2"/>
0489   </ResponseHeader>
0490   <BatchItem>
0491     <Operation type="Enumeration" value="Revoke"/>
0492     <UniqueBatchItemID type="ByteString" value="79b998c5f29465f4"/>
0493     <ResultStatus type="Enumeration" value="Success"/>
0494     <ResponsePayload>
0495       <UniqueIdentifier type="TextString"
0496       value="$UNIQUE_IDENTIFIER_0"/>
0497     </ResponsePayload>
0498   </BatchItem>
0499   <BatchItem>
0500     <Operation type="Enumeration" value="Destroy"/>
0501     <UniqueBatchItemID type="ByteString" value="b0633f0e41187345"/>
0502     <ResultStatus type="Enumeration" value="Success"/>
0503     <ResponsePayload>
0504       <UniqueIdentifier type="TextString"
0505       value="$UNIQUE_IDENTIFIER_0"/>
0506     </ResponsePayload>
0507   </BatchItem>
0508 </ResponseMessage>
```

802

803 2.3.9 TC-61-12 - Import of a Third-party Key

804 This test case tests the import of a foreign key using the Register operation. To validate that the
805 registered key is treated the same as a locally created key, an attribute is added to the key and
806 then modified. Finally, the key is destroyed.

```
0001 # TIME 0
0002 <RequestMessage>
0003   <RequestHeader>
0004     <ProtocolVersion>
0005       <ProtocolVersionMajor type="Integer" value="1"/>
0006       <ProtocolVersionMinor type="Integer" value="2"/>
0007     </ProtocolVersion>
0008     <BatchCount type="Integer" value="1"/>
0009   </RequestHeader>
0010   <BatchItem>
0011     <Operation type="Enumeration" value="Register"/>
0012     <RequestPayload>
0013       <ObjectType type="Enumeration" value="SymmetricKey"/>
0014       <TemplateAttribute>
0015         <Attribute>
0016           <AttributeName type="TextString" value="Cryptographic
0017           Usage Mask"/>
0018           <AttributeValue type="Integer" value="Encrypt"/>
0019         </Attribute>
0020       </TemplateAttribute>
0021     </RequestPayload>
0022   </BatchItem>
0023 </RequestMessage>
```

0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-61-12"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<SymmetricKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="Raw"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString"
	value="0123456789abcdef0123456789abcdef"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0030	<CryptographicLength type="Integer" value="128"/>
0031	</KeyBlock>
0032	</SymmetricKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="2"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="2"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="AddAttribute"/>
0063	<RequestPayload>
0064	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0065	<Attribute>
0066	<AttributeName type="TextString" value="x-provider"/>
0067	<AttributeValue type="TextString" value="unknown"/>
0068	</Attribute>
0069	</RequestPayload>
0070	</BatchItem>
0071	</RequestMessage>

0072	<ResponseMessage>
0073	<ResponseHeader>
0074	<ProtocolVersion>
0075	<ProtocolVersionMajor type="Integer" value="1"/>
0076	<ProtocolVersionMinor type="Integer" value="2"/>
0077	</ProtocolVersion>
0078	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0079	<BatchCount type="Integer" value="1"/>
0080	</ResponseHeader>
0081	<BatchItem>
0082	<Operation type="Enumeration" value="AddAttribute"/>
0083	<ResultStatus type="Enumeration" value="Success"/>
0084	<ResponsePayload>
0085	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0086	<Attribute>
0087	<AttributeName type="TextString" value="x-provider"/>
0088	<AttributeValue type="TextString" value="unknown"/>
0089	</Attribute>
0090	</ResponsePayload>
0091	</BatchItem>
0092	</ResponseMessage>
# TIME 2	
0093	<RequestMessage>
0094	<RequestHeader>
0095	<ProtocolVersion>
0096	<ProtocolVersionMajor type="Integer" value="1"/>
0097	<ProtocolVersionMinor type="Integer" value="2"/>
0098	</ProtocolVersion>
0099	<BatchCount type="Integer" value="1"/>
0100	</RequestHeader>
0101	<BatchItem>
0102	<Operation type="Enumeration" value="ModifyAttribute"/>
0103	<RequestPayload>
0104	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0105	<Attribute>
0106	<AttributeName type="TextString" value="x-provider"/>
0107	<AttributeValue type="TextString" value="third party"/>
0108	</Attribute>
0109	</RequestPayload>
0110	</BatchItem>
0111	</RequestMessage>
0112	<ResponseMessage>
0113	<ResponseHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="2"/>
0117	</ProtocolVersion>
0118	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0119	<BatchCount type="Integer" value="1"/>
0120	</ResponseHeader>
0121	<BatchItem>
0122	<Operation type="Enumeration" value="ModifyAttribute"/>
0123	<ResultStatus type="Enumeration" value="Success"/>
0124	<ResponsePayload>
0125	<UniqueIdentifier type="TextString"

0126	value="\$UNIQUE_IDENTIFIER_0"/>
0127	<Attribute>
0128	<AttributeName type="TextString" value="x-provider"/>
0129	<AttributeValue type="TextString" value="third party"/>
0130	</Attribute>
0131	</ResponsePayload>
0132	</BatchItem>
0133	</ResponseMessage>
0133	# TIME 3
0134	<RequestMessage>
0135	<RequestHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="2"/>
0139	</ProtocolVersion>
0140	<BatchCount type="Integer" value="1"/>
0141	</RequestHeader>
0142	<BatchItem>
0143	<Operation type="Enumeration" value="Destroy"/>
0144	<RequestPayload>
0145	<UniqueIdentifier type="TextString"
0146	value="\$UNIQUE_IDENTIFIER_0"/>
0147	</RequestPayload>
0148	</BatchItem>
0149	</RequestMessage>
0150	<ResponseMessage>
0151	<ResponseHeader>
0152	<ProtocolVersion>
0153	<ProtocolVersionMajor type="Integer" value="1"/>
0154	<ProtocolVersionMinor type="Integer" value="2"/>
0155	</ProtocolVersion>
0156	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0157	<BatchCount type="Integer" value="1"/>
0158	</ResponseHeader>
0159	<BatchItem>
0160	<Operation type="Enumeration" value="Destroy"/>
0161	<ResultStatus type="Enumeration" value="Success"/>
0162	<ResponsePayload>
0163	<UniqueIdentifier type="TextString"
0164	value="\$UNIQUE_IDENTIFIER_0"/>
	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>

807

808 2.3.10 TC-71-12 - Unrecognized Message Extension with Criticality Indicator

809 False

810 A create request is issued and the request contains a Message Extension with the Criticality
811 Indicator set to false. The server does not understand the extension, but since it is non-critical,
812 the create request is processed normally. Subsequently, the created key is deleted.

0001	# TIME 0
0002	<RequestMessage>
	<RequestHeader>

0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Length"/>
0017	<AttributeValue type="Integer" value="128"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Algorithm"/>
0022	<AttributeValue type="Enumeration" value="AES"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Cryptographic
0026	Usage Mask"/>
0027	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="x-ID"/>
0031	<AttributeValue type="TextString" value="TC-71-12"/>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	<MessageExtension>
0036	<VendorIdentification type="TextString" value="Acme"/>
0037	<CriticalityIndicator type="Boolean" value="false"/>
0038	<VendorExtension>
0039	<TLV tag="0x540001" type="TextString" value="na"/>
0040	</VendorExtension>
0041	</MessageExtension>
0042	</BatchItem>
0043	</RequestMessage>
0044	<ResponseMessage>
0045	<ResponseHeader>
0046	<ProtocolVersion>
0047	<ProtocolVersionMajor type="Integer" value="1"/>
0048	<ProtocolVersionMinor type="Integer" value="2"/>
0049	</ProtocolVersion>
0050	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0051	<BatchCount type="Integer" value="1"/>
0052	</ResponseHeader>
0053	<BatchItem>
0054	<Operation type="Enumeration" value="Create"/>
0055	<ResultStatus type="Enumeration" value="Success"/>
	<ResponsePayload>
	<ObjectType type="Enumeration" value="SymmetricKey"/>
	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER 0"/>

0056	</ResponsePayload>
0057	</BatchItem>
0058	</ResponseMessage>
# TIME 1	
0059	<RequestMessage>
0060	<RequestHeader>
0061	<ProtocolVersion>
0062	<ProtocolVersionMajor type="Integer" value="1"/>
0063	<ProtocolVersionMinor type="Integer" value="2"/>
0064	</ProtocolVersion>
0065	<BatchCount type="Integer" value="1"/>
0066	</RequestHeader>
0067	<BatchItem>
0068	<Operation type="Enumeration" value="Destroy"/>
0069	<RequestPayload>
0070	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0071	</RequestPayload>
0072	</BatchItem>
0073	</RequestMessage>
0074	<ResponseMessage>
0075	<ResponseHeader>
0076	<ProtocolVersion>
0077	<ProtocolVersionMajor type="Integer" value="1"/>
0078	<ProtocolVersionMinor type="Integer" value="2"/>
0079	</ProtocolVersion>
0080	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0081	<BatchCount type="Integer" value="1"/>
0082	</ResponseHeader>
0083	<BatchItem>
0084	<Operation type="Enumeration" value="Destroy"/>
0085	<ResultStatus type="Enumeration" value="Success"/>
0086	<ResponsePayload>
0087	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0088	</ResponsePayload>
0089	</BatchItem>
0090	</ResponseMessage>

813

814 2.3.11 TC-72-12 - Unrecognized Message Extension with Criticality Indicator 815 True

816 A create request is issued and the request contains a Message Extension with the Criticality
817 Indicator set to true. The server does not understand the extension, and since it is critical, the
818 create request fails and an error is returned.

# TIME 0	
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>

0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Length"/>
0017	<AttributeValue type="Integer" value="128"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Algorithm"/>
0022	<AttributeValue type="Enumeration" value="AES"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Cryptographic
0026	Usage Mask"/>
0027	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="x-ID"/>
0031	<AttributeValue type="TextString" value="TC-72-12"/>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	<MessageExtension>
0036	<VendorIdentification type="TextString" value="Acme"/>
0037	<CriticalityIndicator type="Boolean" value="true"/>
0038	<VendorExtension>
0039	<TTLV tag="0x540001" type="TextString" value="na"/>
0040	</VendorExtension>
0041	</MessageExtension>
0042	</BatchItem>
0043	</RequestMessage>
0044	<ResponseMessage>
0045	<ResponseHeader>
0046	<ProtocolVersion>
0047	<ProtocolVersionMajor type="Integer" value="1"/>
0048	<ProtocolVersionMinor type="Integer" value="2"/>
0049	</ProtocolVersion>
0050	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0051	<BatchCount type="Integer" value="1"/>
0052	</ResponseHeader>
0053	<BatchItem>
0054	<Operation type="Enumeration" value="Create"/>
0055	<ResultStatus type="Enumeration" value="OperationFailed"/>
0056	<ResultReason type="Enumeration" value="FeatureNotSupported"/>
0057	<ResultMessage type="TextString" value="Critical Message
0058	Extension not recognized"/>
0059	</BatchItem>
0060	</ResponseMessage>

820 2.3.12 TC-81-12 - Create a Key Pair

821 Create a new private/public key pair. Make sure they are linked correctly by issuing Locate
822 commands with the assigned Unique Identifiers. Finally delete both key halves.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="CreateKeyPair"/>
0011	<RequestPayload>
0012	<CommonTemplateAttribute>
0013	<Attribute>
0014	<AttributeName type="TextString" value="Cryptographic
0015	Algorithm"/>
0016	<AttributeValue type="Enumeration" value="RSA"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
0020	Length"/>
0021	<AttributeValue type="Integer" value="1024"/>
0022	</Attribute>
0023	</CommonTemplateAttribute>
0024	<PrivateKeyTemplateAttribute>
0025	<Attribute>
0026	<AttributeName type="TextString" value="Name"/>
0027	<AttributeValue>
0028	<NameValue type="TextString" value="TC-81-12-
0029	privatekey1"/>
0030	<NameType type="Enumeration"
0031	value="UninterpretedTextString"/>
0032	</Attribute>
0033	</Attribute>
0034	<Attribute>
0035	<AttributeName type="TextString" value="Cryptographic
0036	Usage Mask"/>
0037	<AttributeValue type="Integer" value="Sign"/>
0038	</Attribute>
0039	</PrivateKeyTemplateAttribute>
0040	<PublicKeyTemplateAttribute>
0041	<Attribute>
0042	<AttributeName type="TextString" value="Name"/>
0043	<AttributeValue>
	<NameValue type="TextString" value="TC-81-12-
	publickey1"/>
	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
	</Attribute>
	</Attribute>
	</Attribute>

0044	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0045	<AttributeValue type="Integer" value="Verify"/>
0046	</Attribute>
0047	</PublicKeyTemplateAttribute>
0048	</RequestPayload>
0049	</BatchItem>
0050	</RequestMessage>
0051	<ResponseMessage>
0052	<ResponseHeader>
0053	<ProtocolVersion>
0054	<ProtocolVersionMajor type="Integer" value="1"/>
0055	<ProtocolVersionMinor type="Integer" value="2"/>
0056	</ProtocolVersion>
0057	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0058	<BatchCount type="Integer" value="1"/>
0059	</ResponseHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="CreateKeyPair"/>
0062	<ResultStatus type="Enumeration" value="Success"/>
0063	<ResponsePayload>
0064	<PrivateKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0065	<PublicKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
	# TIME 1
0069	<RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="2"/>
0074	</ProtocolVersion>
0075	<BatchCount type="Integer" value="1"/>
0076	</RequestHeader>
0077	<BatchItem>
0078	<Operation type="Enumeration" value="Locate"/>
0079	<RequestPayload>
0080	<Attribute>
0081	<AttributeName type="TextString" value="Object Type"/>
0082	<AttributeValue type="Enumeration" value="PublicKey"/>
0083	</Attribute>
0084	<Attribute>
0085	<AttributeName type="TextString" value="Link"/>
0086	<AttributeValue>
0087	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0088	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0089	</AttributeValue>
0090	</Attribute>
0091	</RequestPayload>
0092	</BatchItem>
0093	</RequestMessage>
0094	<ResponseMessage>

0095	<ResponseHeader>
0096	<ProtocolVersion>
0097	<ProtocolVersionMajor type="Integer" value="1"/>
0098	<ProtocolVersionMinor type="Integer" value="2"/>
0099	</ProtocolVersion>
0100	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0101	<BatchCount type="Integer" value="1"/>
0102	</ResponseHeader>
0103	<BatchItem>
0104	<Operation type="Enumeration" value="Locate"/>
0105	<ResultStatus type="Enumeration" value="Success"/>
0106	<ResponsePayload>
0107	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0108	</ResponsePayload>
0109	</BatchItem>
0110	</ResponseMessage>
	# TIME 2
0111	<RequestMessage>
0112	<RequestHeader>
0113	<ProtocolVersion>
0114	<ProtocolVersionMajor type="Integer" value="1"/>
0115	<ProtocolVersionMinor type="Integer" value="2"/>
0116	</ProtocolVersion>
0117	<BatchCount type="Integer" value="1"/>
0118	</RequestHeader>
0119	<BatchItem>
0120	<Operation type="Enumeration" value="Locate"/>
0121	<RequestPayload>
0122	<Attribute>
0123	<AttributeName type="TextString" value="Object Type"/>
0124	<AttributeValue type="Enumeration" value="PrivateKey"/>
0125	</Attribute>
0126	<Attribute>
0127	<AttributeName type="TextString" value="Link"/>
0128	<AttributeValue>
0129	<LinkType type="Enumeration" value="PublicKeyLink"/>
0130	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0131	</AttributeValue>
0132	</Attribute>
0133	</RequestPayload>
0134	</BatchItem>
0135	</RequestMessage>
0136	<ResponseMessage>
0137	<ResponseHeader>
0138	<ProtocolVersion>
0139	<ProtocolVersionMajor type="Integer" value="1"/>
0140	<ProtocolVersionMinor type="Integer" value="2"/>
0141	</ProtocolVersion>
0142	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0143	<BatchCount type="Integer" value="1"/>
0144	</ResponseHeader>
0145	<BatchItem>
0146	<Operation type="Enumeration" value="Locate"/>
0147	<ResultStatus type="Enumeration" value="Success"/>
0148	<ResponsePayload>

0149	<UniqueIdentifier type="TextString"
0150	value="\$UNIQUE_IDENTIFIER_0"/>
0151	</ResponsePayload>
0152	</BatchItem>
0153	</ResponseMessage>
# TIME 3	
0153	<RequestMessage>
0154	<RequestHeader>
0155	<ProtocolVersion>
0156	<ProtocolVersionMajor type="Integer" value="1"/>
0157	<ProtocolVersionMinor type="Integer" value="2"/>
0158	</ProtocolVersion>
0159	<BatchCount type="Integer" value="1"/>
0160	</RequestHeader>
0161	<BatchItem>
0162	<Operation type="Enumeration" value="Destroy"/>
0163	<RequestPayload>
0164	<UniqueIdentifier type="TextString"
0165	value="\$UNIQUE_IDENTIFIER_0"/>
0166	</RequestPayload>
0167	</BatchItem>
0168	</RequestMessage>
0169	<ResponseMessage>
0170	<ResponseHeader>
0171	<ProtocolVersion>
0172	<ProtocolVersionMajor type="Integer" value="1"/>
0173	<ProtocolVersionMinor type="Integer" value="2"/>
0174	</ProtocolVersion>
0175	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0176	<BatchCount type="Integer" value="1"/>
0177	</ResponseHeader>
0178	<BatchItem>
0179	<Operation type="Enumeration" value="Destroy"/>
0180	<ResultStatus type="Enumeration" value="Success"/>
0181	<ResponsePayload>
0182	<UniqueIdentifier type="TextString"
0183	value="\$UNIQUE_IDENTIFIER_0"/>
0184	</ResponsePayload>
0185	</BatchItem>
0186	</ResponseMessage>
# TIME 4	
0185	<RequestMessage>
0186	<RequestHeader>
0187	<ProtocolVersion>
0188	<ProtocolVersionMajor type="Integer" value="1"/>
0189	<ProtocolVersionMinor type="Integer" value="2"/>
0190	</ProtocolVersion>
0191	<BatchCount type="Integer" value="1"/>
0192	</RequestHeader>
0193	<BatchItem>
0194	<Operation type="Enumeration" value="Destroy"/>
0195	<RequestPayload>
0196	<UniqueIdentifier type="TextString"
0197	value="\$UNIQUE_IDENTIFIER_1"/>
0198	</RequestPayload>
0199	</BatchItem>

0199	</RequestMessage>
0200	<ResponseMessage>
0201	<ResponseHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="2"/>
0205	</ProtocolVersion>
0206	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0207	<BatchCount type="Integer" value="1"/>
0208	</ResponseHeader>
0209	<BatchItem>
0210	<Operation type="Enumeration" value="Destroy"/>
0211	<ResultStatus type="Enumeration" value="Success"/>
0212	<ResponsePayload>
0213	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0214	</ResponsePayload>
0215	</BatchItem>
0216	</ResponseMessage>

823

824 2.3.13 TC-82-12 - Register Both Halves of a Key Pair

825 Register a private key and a public key and set the Link attribute to point to each other. Verify
826 the links were set correctly by locating the keys based on the link attributes, and then delete
827 both objects.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="PrivateKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0016	<AttributeValue type="Integer" value="Sign"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-82-12-
	prikey"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<PrivateKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="PKCS_8"/>
0026	<KeyValue>

0027	<pre> <KeyMaterial type="ByteString" value="30820276020100300d06092a864886f70d0101010500048202603082025c0 2010002818100930451c9ecd94f5bb9da17dd09381bd23be43eca8c7539f301fc8a8 cd5d5274c3e7699dbdc711c97a7aa91e2c50a82bd0b1034f0df493dec16362427e58 acce7f6ce0f9bcc617bbd8c90d0094a2703ba0d09eb19d1005f2fb265526aac75af3 2f8bc782cded2a57f811e03eaf67a944de5e78413dca8f232d074e6dcea4cec9f020 30100010281800b6a7d736199ea48a420e4537ca0c7c046784dcbeaa63baebc0bc13 2787449cde8d7cad0c0c863c0fefb06c3062befc50033ecf87b4e33a9be7bcbcb8f15 11ae215e80deb5d8af2bd31319d7821196640935a0cd67c94599579f2100d65e0388 31fdafb0dbe2bbdac00a696e67e756350e1c99ace11a36dabac3ed3e730960059024 100ddf672fbcc5bda3d73affc4e791e0c03390224405d69ccaabc749faa0dcd4c258 3c71dde8941a7b9aa030f52ef1451466c074d4d338fe677892acd9e10fd35bd02410 0a98fbc3ed6b4c6f860f97165ac2f7bb6f2e2cb192a9abd49795be5bcf37d8ee69a6 e169c24e5c32e4e7fa33265461407f952ba49e204818a2f785f113f922b8b0240253 f9470390d39049303777ddbc9750e9d64849ce0903eae704dc9f589b7680deb9d609 fd5bcd4decdd6f120542e5cff5d76f2a43c8615fb5b3a9213463797aa9024100alddf 023c0cd94c019bb26d09b9e3ca8fa971cb16aa58b9baf79d6081a1dbba452ba53653 e2804ba98ff69e8bb1b3a161ea225ea501463216a8dab9b88a75e5f02406178646e1 12cf79d921a8a843f17f6e7ff974f688122365bf6690cdfc996e1890952eb3820dd1 890ec1c8619e87a2bd38f9d03b37fac742efb748c7885942c39"/> </pre>
0028	<pre></KeyValue></pre>
0029	<pre><CryptographicAlgorithm type="Enumeration" value="RSA"/></pre>
0030	<pre><CryptographicLength type="Integer" value="1024"/></pre>
0031	<pre></KeyBlock></pre>
0032	<pre></PrivateKey></pre>
0033	<pre></RequestPayload></pre>
0034	<pre></BatchItem></pre>
0035	<pre></RequestMessage></pre>
0036	<pre><ResponseMessage></pre>
0037	<pre><ResponseHeader></pre>
0038	<pre><ProtocolVersion></pre>
0039	<pre><ProtocolVersionMajor type="Integer" value="1"/></pre>
0040	<pre><ProtocolVersionMinor type="Integer" value="2"/></pre>
0041	<pre></ProtocolVersion></pre>
0042	<pre><TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/></pre>
0043	<pre><BatchCount type="Integer" value="1"/></pre>
0044	<pre></ResponseHeader></pre>
0045	<pre><BatchItem></pre>
0046	<pre><Operation type="Enumeration" value="Register"/></pre>
0047	<pre><ResultStatus type="Enumeration" value="Success"/></pre>
0048	<pre><ResponsePayload></pre>
0049	<pre><UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/></pre>
0050	<pre></ResponsePayload></pre>
0051	<pre></BatchItem></pre>
0052	<pre></ResponseMessage></pre>
	<pre># TIME 1</pre>
0053	<pre><RequestMessage></pre>
0054	<pre><RequestHeader></pre>
0055	<pre><ProtocolVersion></pre>
0056	<pre><ProtocolVersionMajor type="Integer" value="1"/></pre>
0057	<pre><ProtocolVersionMinor type="Integer" value="2"/></pre>
0058	<pre></ProtocolVersion></pre>
0059	<pre><BatchCount type="Integer" value="1"/></pre>
0060	<pre></RequestHeader></pre>
0061	<pre><BatchItem></pre>
0062	<pre><Operation type="Enumeration" value="Register"/></pre>

0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PublicKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0068	<AttributeValue type="Integer" value="Verify"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>
0073	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0075	</AttributeValue>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-82-12- pubkey"/>
0080	</Attribute>
0081	</TemplateAttribute>
0082	<PublicKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="X_509"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString" value="30819f300d06092a864886f70d010101050003818d0030818902818100930 451c9ecd94f5bb9da17dd09381bd23be43eca8c7539f301fc8a8cd5d5274c3e7699d bdc711c97a7aa91e2c50a82bd0b1034f0df493dec16362427e58acce7f6ce0f9bcc6 17bbd8c90d0094a2703ba0d09eb19d1005f2fb265526aac75af32f8bc782cded2a57 f811e03eaf67a944de5e78413dca8f232d074e6dcea4cec9f0203010001"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0089	<CryptographicLength type="Integer" value="1024"/>
0090	</KeyBlock>
0091	</PublicKey>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="2"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0109	</ResponsePayload>
0110	</BatchItem>

0111	</ResponseMessage>
	# TIME 2
0112	<RequestMessage>
0113	<RequestHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="2"/>
0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="AddAttribute"/>
0122	<RequestPayload>
0123	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Link"/>
0126	<AttributeValue>
0127	<LinkType type="Enumeration" value="PublicKeyLink"/>
0128	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0129	</AttributeValue>
0130	</Attribute>
0131	</RequestPayload>
0132	</BatchItem>
0133	</RequestMessage>
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="2"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="AddAttribute"/>
0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0148	<Attribute>
0149	<AttributeName type="TextString" value="Link"/>
0150	<AttributeValue>
0151	<LinkType type="Enumeration" value="PublicKeyLink"/>
0152	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0153	</AttributeValue>
0154	</Attribute>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
	# TIME 3
0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>

0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="2"/>
0163	</ProtocolVersion>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Locate"/>
0168	<RequestPayload>
0169	<Attribute>
0170	<AttributeName type="TextString" value="Object Type"/>
0171	<AttributeValue type="Enumeration" value="PublicKey"/>
0172	</Attribute>
0173	<Attribute>
0174	<AttributeName type="TextString" value="Link"/>
0175	<AttributeValue>
0176	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0177	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0178	</AttributeValue>
0179	</Attribute>
0180	</RequestPayload>
0181	</BatchItem>
0182	</RequestMessage>
0183	<ResponseMessage>
0184	<ResponseHeader>
0185	<ProtocolVersion>
0186	<ProtocolVersionMajor type="Integer" value="1"/>
0187	<ProtocolVersionMinor type="Integer" value="2"/>
0188	</ProtocolVersion>
0189	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0190	<BatchCount type="Integer" value="1"/>
0191	</ResponseHeader>
0192	<BatchItem>
0193	<Operation type="Enumeration" value="Locate"/>
0194	<ResultStatus type="Enumeration" value="Success"/>
0195	<ResponsePayload>
0196	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0197	</ResponsePayload>
0198	</BatchItem>
0199	</ResponseMessage>
	# TIME 4
0200	<RequestMessage>
0201	<RequestHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="2"/>
0205	</ProtocolVersion>
0206	<BatchCount type="Integer" value="1"/>
0207	</RequestHeader>
0208	<BatchItem>
0209	<Operation type="Enumeration" value="Locate"/>
0210	<RequestPayload>
0211	<Attribute>
0212	<AttributeName type="TextString" value="Object Type"/>
0213	<AttributeValue type="Enumeration" value="PrivateKey"/>
0214	</Attribute>

0215	<Attribute>
0216	<AttributeName type="TextString" value="Link"/>
0217	<AttributeValue>
0218	<LinkType type="Enumeration" value="PublicKeyLink"/>
0219	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0220	</AttributeValue>
0221	</Attribute>
0222	</RequestPayload>
0223	</BatchItem>
0224	</RequestMessage>
0225	<ResponseMessage>
0226	<ResponseHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="2"/>
0230	</ProtocolVersion>
0231	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0232	<BatchCount type="Integer" value="1"/>
0233	</ResponseHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="Locate"/>
0236	<ResultStatus type="Enumeration" value="Success"/>
0237	<ResponsePayload>
0238	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0239	</ResponsePayload>
0240	</BatchItem>
0241	</ResponseMessage>
	# TIME 5
0242	<RequestMessage>
0243	<RequestHeader>
0244	<ProtocolVersion>
0245	<ProtocolVersionMajor type="Integer" value="1"/>
0246	<ProtocolVersionMinor type="Integer" value="2"/>
0247	</ProtocolVersion>
0248	<BatchCount type="Integer" value="1"/>
0249	</RequestHeader>
0250	<BatchItem>
0251	<Operation type="Enumeration" value="Destroy"/>
0252	<RequestPayload>
0253	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0254	</RequestPayload>
0255	</BatchItem>
0256	</RequestMessage>
0257	<ResponseMessage>
0258	<ResponseHeader>
0259	<ProtocolVersion>
0260	<ProtocolVersionMajor type="Integer" value="1"/>
0261	<ProtocolVersionMinor type="Integer" value="2"/>
0262	</ProtocolVersion>
0263	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0264	<BatchCount type="Integer" value="1"/>
0265	</ResponseHeader>
0266	<BatchItem>

0267	<Operation type="Enumeration" value="Destroy"/>
0268	<ResultStatus type="Enumeration" value="Success"/>
0269	<ResponsePayload>
0270	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0271	</ResponsePayload>
0272	</BatchItem>
0273	</ResponseMessage>
	# TIME 6
0274	<RequestMessage>
0275	<RequestHeader>
0276	<ProtocolVersion>
0277	<ProtocolVersionMajor type="Integer" value="1"/>
0278	<ProtocolVersionMinor type="Integer" value="2"/>
0279	</ProtocolVersion>
0280	<BatchCount type="Integer" value="1"/>
0281	</RequestHeader>
0282	<BatchItem>
0283	<Operation type="Enumeration" value="Destroy"/>
0284	<RequestPayload>
0285	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0286	</RequestPayload>
0287	</BatchItem>
0288	</RequestMessage>
0289	<ResponseMessage>
0290	<ResponseHeader>
0291	<ProtocolVersion>
0292	<ProtocolVersionMajor type="Integer" value="1"/>
0293	<ProtocolVersionMinor type="Integer" value="2"/>
0294	</ProtocolVersion>
0295	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0296	<BatchCount type="Integer" value="1"/>
0297	</ResponseHeader>
0298	<BatchItem>
0299	<Operation type="Enumeration" value="Destroy"/>
0300	<ResultStatus type="Enumeration" value="Success"/>
0301	<ResponsePayload>
0302	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0303	</ResponsePayload>
0304	</BatchItem>
0305	</ResponseMessage>

828

829 2.3.14 TC-91-12 - Create a Key, Re-key

830 Create a symmetric key with a specific name, and then use Locate to find the key. After using
831 Re-key to create a new key, verify that the name was removed from the existing key and copied
832 to the new key. Also verify that the key material for the old key is still retrievable. To clean up,
833 both keys are deleted.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>

0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Length"/>
0022	<AttributeValue type="Integer" value="128"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Cryptographic
0026	Usage Mask"/>
0027	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="Name"/>
0031	<AttributeValue type="TextString" value="TC-91-12-rekeyKey"/>
0032	<NameType type="Enumeration"
0033	value="UninterpretedTextString"/>
0034	</AttributeValue>
0035	</Attribute>
0036	</TemplateAttribute>
0037	</RequestPayload>
0038	</BatchItem>
0039	</RequestMessage>
0040	<ResponseMessage>
0041	<ResponseHeader>
0042	<ProtocolVersion>
0043	<ProtocolVersionMajor type="Integer" value="1"/>
0044	<ProtocolVersionMinor type="Integer" value="2"/>
0045	</ProtocolVersion>
0046	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0047	<BatchCount type="Integer" value="1"/>
0048	</ResponseHeader>
0049	<BatchItem>
0050	<Operation type="Enumeration" value="Create"/>
0051	<ResultStatus type="Enumeration" value="Success"/>
0052	<ResponsePayload>
0053	<ObjectType type="Enumeration" value="SymmetricKey"/>
0054	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>

0055	# TIME 1
0056	<RequestMessage>
0057	<RequestHeader>
0058	<ProtocolVersion>
0059	<ProtocolVersionMajor type="Integer" value="1"/>
0060	<ProtocolVersionMinor type="Integer" value="2"/>
0061	</ProtocolVersion>
0062	<BatchCount type="Integer" value="1"/>
0063	</RequestHeader>
0064	<BatchItem>
0065	<Operation type="Enumeration" value="Locate"/>
0066	<RequestPayload>
0067	<Attribute>
0068	<AttributeName type="TextString" value="Name"/>
0069	<AttributeValue>
0070	<NameValue type="TextString" value="TC-91-12-rekeyKey"/>
0071	<NameType type="Enumeration"
0072	value="UninterpretedTextString"/>
0073	</AttributeValue>
0074	</Attribute>
0075	</RequestPayload>
0076	</BatchItem>
0077	</RequestMessage>
0078	<ResponseMessage>
0079	<ResponseHeader>
0080	<ProtocolVersion>
0081	<ProtocolVersionMajor type="Integer" value="1"/>
0082	<ProtocolVersionMinor type="Integer" value="2"/>
0083	</ProtocolVersion>
0084	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0085	<BatchCount type="Integer" value="1"/>
0086	</ResponseHeader>
0087	<BatchItem>
0088	<Operation type="Enumeration" value="Locate"/>
0089	<ResultStatus type="Enumeration" value="Success"/>
0090	<ResponsePayload>
0091	<UniqueIdentifier type="TextString"
0092	value="\$UNIQUE_IDENTIFIER_0"/>
0093	</ResponsePayload>
0094	</BatchItem>
0095	</ResponseMessage>
0096	# TIME 2
0097	<RequestMessage>
0098	<RequestHeader>
0099	<ProtocolVersion>
0100	<ProtocolVersionMajor type="Integer" value="1"/>
0101	<ProtocolVersionMinor type="Integer" value="2"/>
0102	</ProtocolVersion>
0103	<BatchCount type="Integer" value="1"/>
0104	</RequestHeader>
0105	<BatchItem>
0106	<Operation type="Enumeration" value="ReKey"/>
0107	<RequestPayload>
0108	<UniqueIdentifier type="TextString"
0109	value="\$UNIQUE_IDENTIFIER_0"/>
0110	</RequestPayload>
0111	</BatchItem>

0107	</RequestMessage>
0108	<ResponseMessage>
0109	<ResponseHeader>
0110	<ProtocolVersion>
0111	<ProtocolVersionMajor type="Integer" value="1"/>
0112	<ProtocolVersionMinor type="Integer" value="2"/>
0113	</ProtocolVersion>
0114	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0115	<BatchCount type="Integer" value="1"/>
0116	</ResponseHeader>
0117	<BatchItem>
0118	<Operation type="Enumeration" value="ReKey"/>
0119	<ResultStatus type="Enumeration" value="Success"/>
0120	<ResponsePayload>
0121	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0122	</ResponsePayload>
0123	</BatchItem>
0124	</ResponseMessage>
# TIME 3	
0125	<RequestMessage>
0126	<RequestHeader>
0127	<ProtocolVersion>
0128	<ProtocolVersionMajor type="Integer" value="1"/>
0129	<ProtocolVersionMinor type="Integer" value="2"/>
0130	</ProtocolVersion>
0131	<BatchCount type="Integer" value="1"/>
0132	</RequestHeader>
0133	<BatchItem>
0134	<Operation type="Enumeration" value="Locate"/>
0135	<RequestPayload>
0136	<Attribute>
0137	<AttributeName type="TextString" value="Name"/>
0138	<AttributeValue>
0139	<NameValue type="TextString" value="TC-91-12-rekeyKey"/>
0140	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0141	</AttributeValue>
0142	</Attribute>
0143	</RequestPayload>
0144	</BatchItem>
0145	</RequestMessage>
0146	<ResponseMessage>
0147	<ResponseHeader>
0148	<ProtocolVersion>
0149	<ProtocolVersionMajor type="Integer" value="1"/>
0150	<ProtocolVersionMinor type="Integer" value="2"/>
0151	</ProtocolVersion>
0152	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0153	<BatchCount type="Integer" value="1"/>
0154	</ResponseHeader>
0155	<BatchItem>
0156	<Operation type="Enumeration" value="Locate"/>
0157	<ResultStatus type="Enumeration" value="Success"/>
0158	<ResponsePayload>
0159	<UniqueIdentifier type="TextString"

0160	value="\$UNIQUE_IDENTIFIER_1"/>
0161	</ResponsePayload>
0162	</BatchItem>
0162	</ResponseMessage>
# TIME 4	
0163	<RequestMessage>
0164	<RequestHeader>
0165	<ProtocolVersion>
0166	<ProtocolVersionMajor type="Integer" value="1"/>
0167	<ProtocolVersionMinor type="Integer" value="2"/>
0168	</ProtocolVersion>
0169	<BatchCount type="Integer" value="1"/>
0170	</RequestHeader>
0171	<BatchItem>
0172	<Operation type="Enumeration" value="GetAttributes"/>
0173	<RequestPayload>
0174	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0175	<AttributeName type="TextString" value="Name"/>
0176	</RequestPayload>
0177	</BatchItem>
0178	</RequestMessage>
0179	<ResponseMessage>
0180	<ResponseHeader>
0181	<ProtocolVersion>
0182	<ProtocolVersionMajor type="Integer" value="1"/>
0183	<ProtocolVersionMinor type="Integer" value="2"/>
0184	</ProtocolVersion>
0185	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0186	<BatchCount type="Integer" value="1"/>
0187	</ResponseHeader>
0188	<BatchItem>
0189	<Operation type="Enumeration" value="GetAttributes"/>
0190	<ResultStatus type="Enumeration" value="Success"/>
0191	<ResponsePayload>
0192	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0193	</ResponsePayload>
0194	</BatchItem>
0195	</ResponseMessage>
# TIME 5	
0196	<RequestMessage>
0197	<RequestHeader>
0198	<ProtocolVersion>
0199	<ProtocolVersionMajor type="Integer" value="1"/>
0200	<ProtocolVersionMinor type="Integer" value="2"/>
0201	</ProtocolVersion>
0202	<BatchCount type="Integer" value="1"/>
0203	</RequestHeader>
0204	<BatchItem>
0205	<Operation type="Enumeration" value="Get"/>
0206	<RequestPayload>
0207	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0208	</RequestPayload>
0209	</BatchItem>

0210	</RequestMessage>
0211	<ResponseMessage>
0212	<ResponseHeader>
0213	<ProtocolVersion>
0214	<ProtocolVersionMajor type="Integer" value="1"/>
0215	<ProtocolVersionMinor type="Integer" value="2"/>
0216	</ProtocolVersion>
0217	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0218	<BatchCount type="Integer" value="1"/>
0219	</ResponseHeader>
0220	<BatchItem>
0221	<Operation type="Enumeration" value="Get"/>
0222	<ResultStatus type="Enumeration" value="Success"/>
0223	<ResponsePayload>
0224	<ObjectType type="Enumeration" value="SymmetricKey"/>
0225	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0226	<SymmetricKey>
0227	<KeyBlock>
0228	<KeyFormatType type="Enumeration" value="Raw"/>
0229	<KeyValue>
0230	<KeyMaterial type="ByteString"
	value="9ca9840291a65889043c37707da997e8"/>
0231	</KeyMaterial>
0232	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0233	<CryptographicLength type="Integer" value="128"/>
0234	</KeyBlock>
0235	</SymmetricKey>
0236	</ResponsePayload>
0237	</BatchItem>
0238	</ResponseMessage>
	# TIME 6
0239	<RequestMessage>
0240	<RequestHeader>
0241	<ProtocolVersion>
0242	<ProtocolVersionMajor type="Integer" value="1"/>
0243	<ProtocolVersionMinor type="Integer" value="2"/>
0244	</ProtocolVersion>
0245	<BatchCount type="Integer" value="1"/>
0246	</RequestHeader>
0247	<BatchItem>
0248	<Operation type="Enumeration" value="Destroy"/>
0249	<RequestPayload>
0250	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0251	</RequestPayload>
0252	</BatchItem>
0253	</RequestMessage>
0254	<ResponseMessage>
0255	<ResponseHeader>
0256	<ProtocolVersion>
0257	<ProtocolVersionMajor type="Integer" value="1"/>
0258	<ProtocolVersionMinor type="Integer" value="2"/>
0259	</ProtocolVersion>
0260	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0261	<BatchCount type="Integer" value="1"/>

0262	</ResponseHeader>
0263	<BatchItem>
0264	<Operation type="Enumeration" value="Destroy"/>
0265	<ResultStatus type="Enumeration" value="Success"/>
0266	<ResponsePayload>
0267	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0268	</ResponsePayload>
0269	</BatchItem>
0270	</ResponseMessage>
# TIME 7	
0271	<RequestMessage>
0272	<RequestHeader>
0273	<ProtocolVersion>
0274	<ProtocolVersionMajor type="Integer" value="1"/>
0275	<ProtocolVersionMinor type="Integer" value="2"/>
0276	</ProtocolVersion>
0277	<BatchCount type="Integer" value="1"/>
0278	</RequestHeader>
0279	<BatchItem>
0280	<Operation type="Enumeration" value="Destroy"/>
0281	<RequestPayload>
0282	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0283	</RequestPayload>
0284	</BatchItem>
0285	</RequestMessage>
0286	<ResponseMessage>
0287	<ResponseHeader>
0288	<ProtocolVersion>
0289	<ProtocolVersionMajor type="Integer" value="1"/>
0290	<ProtocolVersionMinor type="Integer" value="2"/>
0291	</ProtocolVersion>
0292	<TimeStamp type="DateTime" value="2012-04-27T08:12:26+00:00"/>
0293	<BatchCount type="Integer" value="1"/>
0294	</ResponseHeader>
0295	<BatchItem>
0296	<Operation type="Enumeration" value="Destroy"/>
0297	<ResultStatus type="Enumeration" value="Success"/>
0298	<ResponsePayload>
0299	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0300	</ResponsePayload>
0301	</BatchItem>
0302	</ResponseMessage>

834

835 2.3.15 TC-92-12 - Existing Key Expired, Re-key with Same Life-cycle

836 Create a new symmetric key. Then add the Activation Date and Deactivation Date attributes
837 based on the timestamp in the response to the Create request. The Activation Date is set to the
838 current time and the Deactivation Date to a time in the near future. Repeated Get Attribute calls
839 are performed to verify that the state is first 'Active', then subsequently 'Deactivated'. Then
840 issue a Re-key request, including an Offset value of zero leading to the Activation Date of the
841 replacement key to be set to the same value as the Initial Date of the replacement key. Verify

842 from the response that the Activation Date and Deactivation Date attributes were set correctly
843 (if they are not returned, issue a Get Attribute request). Do a Get Attribute operation to verify
844 that the state of the new key is 'Active'. To clean up, both keys are deleted.

	<i># TIME 0</i>
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="TC-92-12-rekeyKey"/>
0030	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0031	</AttributeValue>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="2"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2012-04-27T08:12:27+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>

0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
	# TIME 1
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="2"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="2"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="AddAttribute"/>
0065	<UniqueBatchItemID type="ByteString" value="606051f958d79b0f"/>
0066	<RequestPayload>
0067	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0068	<Attribute>
0069	<AttributeName type="TextString" value="Activation Date"/>
0070	<AttributeValue type="DateTime" value="\$NOW"/>
0071	</Attribute>
0072	</RequestPayload>
0073	</BatchItem>
0074	<BatchItem>
0075	<Operation type="Enumeration" value="AddAttribute"/>
0076	<UniqueBatchItemID type="ByteString" value="7cb12802f6a52cf1"/>
0077	<RequestPayload>
0078	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0079	<Attribute>
0080	<AttributeName type="TextString" value="Deactivation Date"/>
0081	<AttributeValue type="DateTime" value="\$NOW+120"/>
0082	</Attribute>
0083	</RequestPayload>
0084	</BatchItem>
0085	</RequestMessage>
0086	<ResponseMessage>
0087	<ResponseHeader>
0088	<ProtocolVersion>
0089	<ProtocolVersionMajor type="Integer" value="1"/>
0090	<ProtocolVersionMinor type="Integer" value="2"/>
0091	</ProtocolVersion>
0092	<TimeStamp type="DateTime" value="2012-04-27T08:12:27+00:00"/>
0093	<BatchCount type="Integer" value="2"/>
0094	</ResponseHeader>
0095	<BatchItem>
0096	<Operation type="Enumeration" value="AddAttribute"/>
0097	<UniqueBatchItemID type="ByteString" value="606051f958d79b0f"/>
0098	<ResultStatus type="Enumeration" value="Success"/>
0099	<ResponsePayload>
0100	<UniqueIdentifier type="TextString"

0101	value="\$UNIQUE_IDENTIFIER_0"/>
0102	<Attribute>
0103	<AttributeName type="TextString" value="Activation Date"/>
0104	<AttributeValue type="DateTime" value="\$NOW"/>
0105	</Attribute>
0106	</ResponsePayload>
0107	</BatchItem>
0108	<BatchItem>
0109	<Operation type="Enumeration" value="AddAttribute"/>
0110	<UniqueBatchItemID type="ByteString" value="7cb12802f6a52cf1"/>
0111	<ResultStatus type="Enumeration" value="Success"/>
0112	<ResponsePayload>
0113	<UniqueIdentifier type="TextString"
0114	value="\$UNIQUE_IDENTIFIER_0"/>
0115	<Attribute>
0116	<AttributeName type="TextString" value="Deactivation Date"/>
0117	<AttributeValue type="DateTime" value="\$NOW+120"/>
0118	</Attribute>
0119	</ResponsePayload>
0120	</BatchItem>
0121	</ResponseMessage>
0122	# TIME 2
0123	<RequestMessage>
0124	<RequestHeader>
0125	<ProtocolVersion>
0126	<ProtocolVersionMajor type="Integer" value="1"/>
0127	<ProtocolVersionMinor type="Integer" value="2"/>
0128	</ProtocolVersion>
0129	<BatchCount type="Integer" value="1"/>
0130	</RequestHeader>
0131	<BatchItem>
0132	<Operation type="Enumeration" value="GetAttributes"/>
0133	<RequestPayload>
0134	<UniqueIdentifier type="TextString"
0135	value="\$UNIQUE_IDENTIFIER_0"/>
0136	<AttributeName type="TextString" value="State"/>
0137	</RequestPayload>
0138	</BatchItem>
0139	</RequestMessage>
0140	<ResponseMessage>
0141	<ResponseHeader>
0142	<ProtocolVersion>
0143	<ProtocolVersionMajor type="Integer" value="1"/>
0144	<ProtocolVersionMinor type="Integer" value="2"/>
0145	</ProtocolVersion>
0146	<TimeStamp type="DateTime" value="2012-04-27T08:12:27+00:00"/>
0147	<BatchCount type="Integer" value="1"/>
0148	</ResponseHeader>
0149	<BatchItem>
0150	<Operation type="Enumeration" value="GetAttributes"/>
0151	<ResultStatus type="Enumeration" value="Success"/>
0152	<ResponsePayload>
	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
	<Attribute>
	<AttributeName type="TextString" value="State"/>
	<AttributeValue type="Enumeration" value="Active"/>

0153	</Attribute>
0154	</ResponsePayload>
0155	</BatchItem>
0156	</ResponseMessage>
	<i># TIME 3</i>
	<i># [REPEAT] until GetAttributes response shows State changed to Deactivated</i>
0157	<RequestMessage>
0158	<RequestHeader>
0159	<ProtocolVersion>
0160	<ProtocolVersionMajor type="Integer" value="1"/>
0161	<ProtocolVersionMinor type="Integer" value="2"/>
0162	</ProtocolVersion>
0163	<BatchCount type="Integer" value="1"/>
0164	</RequestHeader>
0165	<BatchItem>
0166	<Operation type="Enumeration" value="GetAttributes"/>
0167	<RequestPayload>
0168	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0169	<AttributeName type="TextString" value="State"/>
0170	</RequestPayload>
0171	</BatchItem>
0172	</RequestMessage>
0173	<ResponseMessage>
0174	<ResponseHeader>
0175	<ProtocolVersion>
0176	<ProtocolVersionMajor type="Integer" value="1"/>
0177	<ProtocolVersionMinor type="Integer" value="2"/>
0178	</ProtocolVersion>
0179	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0180	<BatchCount type="Integer" value="1"/>
0181	</ResponseHeader>
0182	<BatchItem>
0183	<Operation type="Enumeration" value="GetAttributes"/>
0184	<ResultStatus type="Enumeration" value="Success"/>
0185	<ResponsePayload>
0186	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0187	<Attribute>
0188	<AttributeName type="TextString" value="State"/>
0189	<AttributeValue type="Enumeration" value="Deactivated"/>
0190	</Attribute>
0191	</ResponsePayload>
0192	</BatchItem>
0193	</ResponseMessage>
	<i># TIME 4</i>
0194	<RequestMessage>
0195	<RequestHeader>
0196	<ProtocolVersion>
0197	<ProtocolVersionMajor type="Integer" value="1"/>
0198	<ProtocolVersionMinor type="Integer" value="2"/>
0199	</ProtocolVersion>
0200	<BatchCount type="Integer" value="1"/>
0201	</RequestHeader>
0202	<BatchItem>

0203	<Operation type="Enumeration" value="ReKey"/>
0204	<RequestPayload>
0205	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0206	<Offset type="Interval" value="0"/>
0207	</RequestPayload>
0208	</BatchItem>
0209	</RequestMessage>
0210	<ResponseMessage>
0211	<ResponseHeader>
0212	<ProtocolVersion>
0213	<ProtocolVersionMajor type="Integer" value="1"/>
0214	<ProtocolVersionMinor type="Integer" value="2"/>
0215	</ProtocolVersion>
0216	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0217	<BatchCount type="Integer" value="1"/>
0218	</ResponseHeader>
0219	<BatchItem>
0220	<Operation type="Enumeration" value="ReKey"/>
0221	<ResultStatus type="Enumeration" value="Success"/>
0222	<ResponsePayload>
0223	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0224	</ResponsePayload>
0225	</BatchItem>
0226	</ResponseMessage>
	# TIME 5
0227	<RequestMessage>
0228	<RequestHeader>
0229	<ProtocolVersion>
0230	<ProtocolVersionMajor type="Integer" value="1"/>
0231	<ProtocolVersionMinor type="Integer" value="2"/>
0232	</ProtocolVersion>
0233	<BatchCount type="Integer" value="1"/>
0234	</RequestHeader>
0235	<BatchItem>
0236	<Operation type="Enumeration" value="GetAttributes"/>
0237	<RequestPayload>
0238	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0239	<AttributeName type="TextString" value="Activation Date"/>
0240	<AttributeName type="TextString" value="Deactivation Date"/>
0241	</RequestPayload>
0242	</BatchItem>
0243	</RequestMessage>
0244	<ResponseMessage>
0245	<ResponseHeader>
0246	<ProtocolVersion>
0247	<ProtocolVersionMajor type="Integer" value="1"/>
0248	<ProtocolVersionMinor type="Integer" value="2"/>
0249	</ProtocolVersion>
0250	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0251	<BatchCount type="Integer" value="1"/>
0252	</ResponseHeader>
0253	<BatchItem>
0254	<Operation type="Enumeration" value="GetAttributes"/>

0255	<ResultStatus type="Enumeration" value="Success"/>
0256	<ResponsePayload>
0257	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0258	<Attribute>
0259	<AttributeName type="TextString" value="Activation Date"/>
0260	<AttributeValue type="DateTime" value="\$NOW"/>
0261	</Attribute>
0262	<Attribute>
0263	<AttributeName type="TextString" value="Deactivation Date"/>
0264	<AttributeValue type="DateTime" value="\$NOW+120"/>
0265	</Attribute>
0266	</ResponsePayload>
0267	</BatchItem>
0268	</ResponseMessage>
	# TIME 6
0269	<RequestMessage>
0270	<RequestHeader>
0271	<ProtocolVersion>
0272	<ProtocolVersionMajor type="Integer" value="1"/>
0273	<ProtocolVersionMinor type="Integer" value="2"/>
0274	</ProtocolVersion>
0275	<BatchCount type="Integer" value="1"/>
0276	</RequestHeader>
0277	<BatchItem>
0278	<Operation type="Enumeration" value="GetAttributes"/>
0279	<RequestPayload>
0280	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0281	<AttributeName type="TextString" value="State"/>
0282	</RequestPayload>
0283	</BatchItem>
0284	</RequestMessage>
0285	<ResponseMessage>
0286	<ResponseHeader>
0287	<ProtocolVersion>
0288	<ProtocolVersionMajor type="Integer" value="1"/>
0289	<ProtocolVersionMinor type="Integer" value="2"/>
0290	</ProtocolVersion>
0291	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0292	<BatchCount type="Integer" value="1"/>
0293	</ResponseHeader>
0294	<BatchItem>
0295	<Operation type="Enumeration" value="GetAttributes"/>
0296	<ResultStatus type="Enumeration" value="Success"/>
0297	<ResponsePayload>
0298	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0299	<Attribute>
0300	<AttributeName type="TextString" value="State"/>
0301	<AttributeValue type="Enumeration" value="Active"/>
0302	</Attribute>
0303	</ResponsePayload>
0304	</BatchItem>
0305	</ResponseMessage>
	# TIME 7

0306	<RequestMessage>
0307	<RequestHeader>
0308	<ProtocolVersion>
0309	<ProtocolVersionMajor type="Integer" value="1"/>
0310	<ProtocolVersionMinor type="Integer" value="2"/>
0311	</ProtocolVersion>
0312	<BatchCount type="Integer" value="1"/>
0313	</RequestHeader>
0314	<BatchItem>
0315	<Operation type="Enumeration" value="Destroy"/>
0316	<RequestPayload>
0317	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0318	</RequestPayload>
0319	</BatchItem>
0320	</RequestMessage>
0321	<ResponseMessage>
0322	<ResponseHeader>
0323	<ProtocolVersion>
0324	<ProtocolVersionMajor type="Integer" value="1"/>
0325	<ProtocolVersionMinor type="Integer" value="2"/>
0326	</ProtocolVersion>
0327	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0328	<BatchCount type="Integer" value="1"/>
0329	</ResponseHeader>
0330	<BatchItem>
0331	<Operation type="Enumeration" value="Destroy"/>
0332	<ResultStatus type="Enumeration" value="Success"/>
0333	<ResponsePayload>
0334	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0335	</ResponsePayload>
0336	</BatchItem>
0337	</ResponseMessage>
	# TIME 8
0338	<RequestMessage>
0339	<RequestHeader>
0340	<ProtocolVersion>
0341	<ProtocolVersionMajor type="Integer" value="1"/>
0342	<ProtocolVersionMinor type="Integer" value="2"/>
0343	</ProtocolVersion>
0344	<BatchOrderOption type="Boolean" value="true"/>
0345	<BatchCount type="Integer" value="2"/>
0346	</RequestHeader>
0347	<BatchItem>
0348	<Operation type="Enumeration" value="Revoke"/>
0349	<UniqueBatchItemID type="ByteString" value="955dfbb9abbec308"/>
0350	<RequestPayload>
0351	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0352	<RevocationReason>
0353	<RevocationReasonCode type="Enumeration"
	value="CessationOfOperation"/>
0354	</RevocationReason>
0355	</RequestPayload>
0356	</BatchItem>
0357	<BatchItem>

0358	<Operation type="Enumeration" value="Destroy"/>
0359	<UniqueBatchItemID type="ByteString" value="6ce5ea0c8334b076"/>
0360	<RequestPayload>
0361	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0362	</RequestPayload>
0363	</BatchItem>
0364	</RequestMessage>
0365	<ResponseMessage>
0366	<ResponseHeader>
0367	<ProtocolVersion>
0368	<ProtocolVersionMajor type="Integer" value="1"/>
0369	<ProtocolVersionMinor type="Integer" value="2"/>
0370	</ProtocolVersion>
0371	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0372	<BatchCount type="Integer" value="2"/>
0373	</ResponseHeader>
0374	<BatchItem>
0375	<Operation type="Enumeration" value="Revoke"/>
0376	<UniqueBatchItemID type="ByteString" value="955dfbb9abbec308"/>
0377	<ResultStatus type="Enumeration" value="Success"/>
0378	<ResponsePayload>
0379	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0380	</ResponsePayload>
0381	</BatchItem>
0382	<BatchItem>
0383	<Operation type="Enumeration" value="Destroy"/>
0384	<UniqueBatchItemID type="ByteString" value="6ce5ea0c8334b076"/>
0385	<ResultStatus type="Enumeration" value="Success"/>
0386	<ResponsePayload>
0387	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0388	</ResponsePayload>
0389	</BatchItem>
0390	</ResponseMessage>

845

846 2.3.16 TC-93-12 - Existing Key Compromised, Re-key with Same Life-cycle

847 Create a new symmetric key with the Activation Date in the past. Do a Get Attribute operation
848 on the State attribute to verify the key is 'Active'. Then revoke the key as compromised, verify
849 that the state has changed to 'Compromised'. Create a replacement key using Re-key with the
850 offset set to '0' to indicate that the times are to be copied from the existing key. Do a Get
851 Attribute operation to verify that the state of the new key is 'Active'. To clean up, both keys are
852 deleted.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>

0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Length"/>
0022	<AttributeValue type="Integer" value="128"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Cryptographic
0026	Usage Mask"/>
0027	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="Activation Date"/>
0031	<AttributeValue type="DateTime" value="\$NOW"/>
0032	</Attribute>
0033	<Attribute>
0034	<AttributeName type="TextString" value="Name"/>
0035	<AttributeValue type="TextString" value="TC-93-12-rekeyKey"/>
0036	<NameType type="Enumeration"
0037	value="UninterpretedTextString"/>
0038	</AttributeValue>
0039	</Attribute>
0040	</TemplateAttribute>
0041	</RequestPayload>
0042	</BatchItem>
0043	</RequestMessage>
0044	<ResponseMessage>
0045	<ResponseHeader>
0046	<ProtocolVersion>
0047	<ProtocolVersionMajor type="Integer" value="1"/>
0048	<ProtocolVersionMinor type="Integer" value="2"/>
0049	</ProtocolVersion>
0050	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0051	<BatchCount type="Integer" value="1"/>
0052	</ResponseHeader>
0053	<BatchItem>
0054	<Operation type="Enumeration" value="Create"/>
0055	<ResultStatus type="Enumeration" value="Success"/>
0056	<ResponsePayload>
0057	<ObjectType type="Enumeration" value="SymmetricKey"/>
0058	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>
	# TIME 1

0059	<RequestMessage>
0060	<RequestHeader>
0061	<ProtocolVersion>
0062	<ProtocolVersionMajor type="Integer" value="1"/>
0063	<ProtocolVersionMinor type="Integer" value="2"/>
0064	</ProtocolVersion>
0065	<BatchCount type="Integer" value="1"/>
0066	</RequestHeader>
0067	<BatchItem>
0068	<Operation type="Enumeration" value="GetAttributes"/>
0069	<RequestPayload>
0070	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0071	<AttributeName type="TextString" value="State"/>
0072	</RequestPayload>
0073	</BatchItem>
0074	</RequestMessage>
0075	<ResponseMessage>
0076	<ResponseHeader>
0077	<ProtocolVersion>
0078	<ProtocolVersionMajor type="Integer" value="1"/>
0079	<ProtocolVersionMinor type="Integer" value="2"/>
0080	</ProtocolVersion>
0081	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0082	<BatchCount type="Integer" value="1"/>
0083	</ResponseHeader>
0084	<BatchItem>
0085	<Operation type="Enumeration" value="GetAttributes"/>
0086	<ResultStatus type="Enumeration" value="Success"/>
0087	<ResponsePayload>
0088	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0089	<Attribute>
0090	<AttributeName type="TextString" value="State"/>
0091	<AttributeValue type="Enumeration" value="Active"/>
0092	</Attribute>
0093	</ResponsePayload>
0094	</BatchItem>
0095	</ResponseMessage>
	# TIME 2
0096	<RequestMessage>
0097	<RequestHeader>
0098	<ProtocolVersion>
0099	<ProtocolVersionMajor type="Integer" value="1"/>
0100	<ProtocolVersionMinor type="Integer" value="2"/>
0101	</ProtocolVersion>
0102	<BatchCount type="Integer" value="1"/>
0103	</RequestHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Revoke"/>
0106	<RequestPayload>
0107	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0108	<RevocationReason>
0109	<RevocationReasonCode type="Enumeration"
	value="KeyCompromise"/>
0110	</RevocationReason>

0111	<CompromiseOccurrenceDate type="DateTime" value="\$NOW"/>
0112	</RequestPayload>
0113	</BatchItem>
0114	</RequestMessage>
0115	<ResponseMessage>
0116	<ResponseHeader>
0117	<ProtocolVersion>
0118	<ProtocolVersionMajor type="Integer" value="1"/>
0119	<ProtocolVersionMinor type="Integer" value="2"/>
0120	</ProtocolVersion>
0121	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0122	<BatchCount type="Integer" value="1"/>
0123	</ResponseHeader>
0124	<BatchItem>
0125	<Operation type="Enumeration" value="Revoke"/>
0126	<ResultStatus type="Enumeration" value="Success"/>
0127	<ResponsePayload>
0128	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0129	</ResponsePayload>
0130	</BatchItem>
0131	</ResponseMessage>
	# TIME 3
0132	<RequestMessage>
0133	<RequestHeader>
0134	<ProtocolVersion>
0135	<ProtocolVersionMajor type="Integer" value="1"/>
0136	<ProtocolVersionMinor type="Integer" value="2"/>
0137	</ProtocolVersion>
0138	<BatchCount type="Integer" value="1"/>
0139	</RequestHeader>
0140	<BatchItem>
0141	<Operation type="Enumeration" value="GetAttributes"/>
0142	<RequestPayload>
0143	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0144	<AttributeName type="TextString" value="State"/>
0145	</RequestPayload>
0146	</BatchItem>
0147	</RequestMessage>
0148	<ResponseMessage>
0149	<ResponseHeader>
0150	<ProtocolVersion>
0151	<ProtocolVersionMajor type="Integer" value="1"/>
0152	<ProtocolVersionMinor type="Integer" value="2"/>
0153	</ProtocolVersion>
0154	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0155	<BatchCount type="Integer" value="1"/>
0156	</ResponseHeader>
0157	<BatchItem>
0158	<Operation type="Enumeration" value="GetAttributes"/>
0159	<ResultStatus type="Enumeration" value="Success"/>
0160	<ResponsePayload>
0161	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0162	<Attribute>

0163	<AttributeName type="TextString" value="State"/>
0164	<AttributeValue type="Enumeration" value="Compromised"/>
0165	</Attribute>
0166	</ResponsePayload>
0167	</BatchItem>
0168	</ResponseMessage>
# TIME 4	
0169	<RequestMessage>
0170	<RequestHeader>
0171	<ProtocolVersion>
0172	<ProtocolVersionMajor type="Integer" value="1"/>
0173	<ProtocolVersionMinor type="Integer" value="2"/>
0174	</ProtocolVersion>
0175	<BatchCount type="Integer" value="1"/>
0176	</RequestHeader>
0177	<BatchItem>
0178	<Operation type="Enumeration" value="ReKey"/>
0179	<RequestPayload>
0180	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0181	</RequestPayload>
0182	</BatchItem>
0183	</RequestMessage>
0184	<ResponseMessage>
0185	<ResponseHeader>
0186	<ProtocolVersion>
0187	<ProtocolVersionMajor type="Integer" value="1"/>
0188	<ProtocolVersionMinor type="Integer" value="2"/>
0189	</ProtocolVersion>
0190	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0191	<BatchCount type="Integer" value="1"/>
0192	</ResponseHeader>
0193	<BatchItem>
0194	<Operation type="Enumeration" value="ReKey"/>
0195	<ResultStatus type="Enumeration" value="Success"/>
0196	<ResponsePayload>
0197	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0198	</ResponsePayload>
0199	</BatchItem>
0200	</ResponseMessage>
# TIME 5	
0201	<RequestMessage>
0202	<RequestHeader>
0203	<ProtocolVersion>
0204	<ProtocolVersionMajor type="Integer" value="1"/>
0205	<ProtocolVersionMinor type="Integer" value="2"/>
0206	</ProtocolVersion>
0207	<BatchCount type="Integer" value="1"/>
0208	</RequestHeader>
0209	<BatchItem>
0210	<Operation type="Enumeration" value="GetAttributes"/>
0211	<RequestPayload>
0212	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0213	<AttributeName type="TextString" value="State"/>

0214	</RequestPayload>
0215	</BatchItem>
0216	</RequestMessage>
0217	<ResponseMessage>
0218	<ResponseHeader>
0219	<ProtocolVersion>
0220	<ProtocolVersionMajor type="Integer" value="1"/>
0221	<ProtocolVersionMinor type="Integer" value="2"/>
0222	</ProtocolVersion>
0223	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0224	<BatchCount type="Integer" value="1"/>
0225	</ResponseHeader>
0226	<BatchItem>
0227	<Operation type="Enumeration" value="GetAttributes"/>
0228	<ResultStatus type="Enumeration" value="Success"/>
0229	<ResponsePayload>
0230	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0231	<Attribute>
0232	<AttributeName type="TextString" value="State"/>
0233	<AttributeValue type="Enumeration" value="Active"/>
0234	</Attribute>
0235	</ResponsePayload>
0236	</BatchItem>
0237	</ResponseMessage>
# TIME 6	
0238	<RequestMessage>
0239	<RequestHeader>
0240	<ProtocolVersion>
0241	<ProtocolVersionMajor type="Integer" value="1"/>
0242	<ProtocolVersionMinor type="Integer" value="2"/>
0243	</ProtocolVersion>
0244	<BatchCount type="Integer" value="1"/>
0245	</RequestHeader>
0246	<BatchItem>
0247	<Operation type="Enumeration" value="Destroy"/>
0248	<RequestPayload>
0249	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0250	</RequestPayload>
0251	</BatchItem>
0252	</RequestMessage>
0253	<ResponseMessage>
0254	<ResponseHeader>
0255	<ProtocolVersion>
0256	<ProtocolVersionMajor type="Integer" value="1"/>
0257	<ProtocolVersionMinor type="Integer" value="2"/>
0258	</ProtocolVersion>
0259	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0260	<BatchCount type="Integer" value="1"/>
0261	</ResponseHeader>
0262	<BatchItem>
0263	<Operation type="Enumeration" value="Destroy"/>
0264	<ResultStatus type="Enumeration" value="Success"/>
0265	<ResponsePayload>
0266	<UniqueIdentifier type="TextString"

0267	value="\$UNIQUE_IDENTIFIER_0"/>
0268	</ResponsePayload>
0269	</BatchItem>
	</ResponseMessage>
0270	# TIME 7
0271	<RequestMessage>
0272	<RequestHeader>
0273	<ProtocolVersion>
0274	<ProtocolVersionMajor type="Integer" value="1"/>
0275	<ProtocolVersionMinor type="Integer" value="2"/>
0276	</ProtocolVersion>
0277	<BatchOrderOption type="Boolean" value="true"/>
0278	<BatchCount type="Integer" value="2"/>
0279	</RequestHeader>
0280	<BatchItem>
0281	<Operation type="Enumeration" value="Revoke"/>
0282	<UniqueBatchItemID type="ByteString" value="c95bbfd6ad466474"/>
0283	<RequestPayload>
0284	<UniqueIdentifier type="TextString"
0285	value="\$UNIQUE_IDENTIFIER_1"/>
0286	<RevocationReason>
0287	<RevocationReasonCode type="Enumeration"
0288	value="CessationOfOperation"/>
0289	</RevocationReason>
0290	</RequestPayload>
0291	</BatchItem>
0292	<BatchItem>
0293	<Operation type="Enumeration" value="Destroy"/>
0294	<UniqueBatchItemID type="ByteString" value="4e6a3e943e1dda87"/>
0295	<RequestPayload>
0296	<UniqueIdentifier type="TextString"
0297	value="\$UNIQUE_IDENTIFIER_1"/>
0298	</RequestPayload>
0299	</BatchItem>
0300	</RequestMessage>
0301	<ResponseMessage>
0302	<ResponseHeader>
0303	<ProtocolVersion>
0304	<ProtocolVersionMajor type="Integer" value="1"/>
0305	<ProtocolVersionMinor type="Integer" value="2"/>
0306	</ProtocolVersion>
0307	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0308	<BatchCount type="Integer" value="2"/>
0309	</ResponseHeader>
0310	<BatchItem>
0311	<Operation type="Enumeration" value="Revoke"/>
0312	<UniqueBatchItemID type="ByteString" value="c95bbfd6ad466474"/>
0313	<ResultStatus type="Enumeration" value="Success"/>
0314	<ResponsePayload>
0315	<UniqueIdentifier type="TextString"
0316	value="\$UNIQUE_IDENTIFIER_1"/>
0317	</ResponsePayload>
	</BatchItem>
	<BatchItem>
	<Operation type="Enumeration" value="Destroy"/>
	<UniqueBatchItemID type="ByteString" value="4e6a3e943e1dda87"/>
	<ResultStatus type="Enumeration" value="Success"/>

0318	<ResponsePayload>
0319	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0320	</ResponsePayload>
0321	</BatchItem>
0322	</ResponseMessage>

853

854 2.3.17 TC-94-12 - Create Key, Re-key with New Life-cycle

855 Create a symmetric key with a specific name, then use Locate to find the key. After using Re-key
856 to create a new key, verify that the name was removed from the existing key and copied to the
857 new key. To clean up, both keys are deleted.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="TC-94-12-rekeyKey"/>
0030	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0031	</AttributeValue>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	<ResponseMessage>

0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="2"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
	# TIME 1
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="2"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="Locate"/>
0065	<RequestPayload>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Name"/>
0068	<AttributeValue>
0069	<NameValue type="TextString" value="TC-94-12-rekeyKey"/>
0070	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0071	</AttributeValue>
0072	</Attribute>
0073	</RequestPayload>
0074	</BatchItem>
0075	</RequestMessage>
0076	<ResponseMessage>
0077	<ResponseHeader>
0078	<ProtocolVersion>
0079	<ProtocolVersionMajor type="Integer" value="1"/>
0080	<ProtocolVersionMinor type="Integer" value="2"/>
0081	</ProtocolVersion>
0082	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0083	<BatchCount type="Integer" value="1"/>
0084	</ResponseHeader>
0085	<BatchItem>
0086	<Operation type="Enumeration" value="Locate"/>
0087	<ResultStatus type="Enumeration" value="Success"/>
0088	<ResponsePayload>
0089	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0090	</ResponsePayload>

0091	</BatchItem>
0092	</ResponseMessage>
# TIME 2	
0093	<RequestMessage>
0094	<RequestHeader>
0095	<ProtocolVersion>
0096	<ProtocolVersionMajor type="Integer" value="1"/>
0097	<ProtocolVersionMinor type="Integer" value="2"/>
0098	</ProtocolVersion>
0099	<BatchCount type="Integer" value="1"/>
0100	</RequestHeader>
0101	<BatchItem>
0102	<Operation type="Enumeration" value="ReKey"/>
0103	<RequestPayload>
0104	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0105	<TemplateAttribute>
0106	<Attribute>
0107	<AttributeName type="TextString" value="Activation Date"/>
0108	<AttributeValue type="DateTime" value="\$NOW-31536000"/>
0109	</Attribute>
0110	<Attribute>
0111	<AttributeName type="TextString" value="Process Start
	Date"/>
0112	<AttributeValue type="DateTime" value="\$NOW-31536000"/>
0113	</Attribute>
0114	<Attribute>
0115	<AttributeName type="TextString" value="Protect Stop
	Date"/>
0116	<AttributeValue type="DateTime" value="\$NOW+31536000"/>
0117	</Attribute>
0118	<Attribute>
0119	<AttributeName type="TextString" value="Deactivation
	Date"/>
0120	<AttributeValue type="DateTime" value="\$NOW+31536000"/>
0121	</Attribute>
0122	</TemplateAttribute>
0123	</RequestPayload>
0124	</BatchItem>
0125	</RequestMessage>
0126	<ResponseMessage>
0127	<ResponseHeader>
0128	<ProtocolVersion>
0129	<ProtocolVersionMajor type="Integer" value="1"/>
0130	<ProtocolVersionMinor type="Integer" value="2"/>
0131	</ProtocolVersion>
0132	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0133	<BatchCount type="Integer" value="1"/>
0134	</ResponseHeader>
0135	<BatchItem>
0136	<Operation type="Enumeration" value="ReKey"/>
0137	<ResultStatus type="Enumeration" value="Success"/>
0138	<ResponsePayload>
0139	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0140	</ResponsePayload>
0141	</BatchItem>

0142	</ResponseMessage>
	# TIME 3
0143	<RequestMessage>
0144	<RequestHeader>
0145	<ProtocolVersion>
0146	<ProtocolVersionMajor type="Integer" value="1"/>
0147	<ProtocolVersionMinor type="Integer" value="2"/>
0148	</ProtocolVersion>
0149	<BatchCount type="Integer" value="1"/>
0150	</RequestHeader>
0151	<BatchItem>
0152	<Operation type="Enumeration" value="GetAttributes"/>
0153	<RequestPayload>
0154	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0155	<AttributeName type="TextString" value="Name"/>
0156	</RequestPayload>
0157	</BatchItem>
0158	</RequestMessage>
0159	<ResponseMessage>
0160	<ResponseHeader>
0161	<ProtocolVersion>
0162	<ProtocolVersionMajor type="Integer" value="1"/>
0163	<ProtocolVersionMinor type="Integer" value="2"/>
0164	</ProtocolVersion>
0165	<TimeStamp type="DateTime" value="2012-04-27T08:14:27+00:00"/>
0166	<BatchCount type="Integer" value="1"/>
0167	</ResponseHeader>
0168	<BatchItem>
0169	<Operation type="Enumeration" value="GetAttributes"/>
0170	<ResultStatus type="Enumeration" value="Success"/>
0171	<ResponsePayload>
0172	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0173	</ResponsePayload>
0174	</BatchItem>
0175	</ResponseMessage>
	# TIME 4
0176	<RequestMessage>
0177	<RequestHeader>
0178	<ProtocolVersion>
0179	<ProtocolVersionMajor type="Integer" value="1"/>
0180	<ProtocolVersionMinor type="Integer" value="2"/>
0181	</ProtocolVersion>
0182	<BatchCount type="Integer" value="1"/>
0183	</RequestHeader>
0184	<BatchItem>
0185	<Operation type="Enumeration" value="GetAttributes"/>
0186	<RequestPayload>
0187	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0188	<AttributeName type="TextString" value="Activation Date"/>
0189	<AttributeName type="TextString" value="Process Start Date"/>
0190	<AttributeName type="TextString" value="Protect Stop Date"/>
0191	<AttributeName type="TextString" value="Deactivation Date"/>
0192	</RequestPayload>

0193	</BatchItem>
0194	</RequestMessage>
0195	<ResponseMessage>
0196	<ResponseHeader>
0197	<ProtocolVersion>
0198	<ProtocolVersionMajor type="Integer" value="1"/>
0199	<ProtocolVersionMinor type="Integer" value="2"/>
0200	</ProtocolVersion>
0201	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0202	<BatchCount type="Integer" value="1"/>
0203	</ResponseHeader>
0204	<BatchItem>
0205	<Operation type="Enumeration" value="GetAttributes"/>
0206	<ResultStatus type="Enumeration" value="Success"/>
0207	<ResponsePayload>
0208	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0209	<Attribute>
0210	<AttributeName type="TextString" value="Activation Date"/>
0211	<AttributeValue type="DateTime" value="\$NOW-31536000"/>
0212	</Attribute>
0213	<Attribute>
0214	<AttributeName type="TextString" value="Process Start
	Date"/>
0215	<AttributeValue type="DateTime" value="\$NOW-31536000"/>
0216	</Attribute>
0217	<Attribute>
0218	<AttributeName type="TextString" value="Protect Stop Date"/>
0219	<AttributeValue type="DateTime" value="\$NOW+31536000"/>
0220	</Attribute>
0221	<Attribute>
0222	<AttributeName type="TextString" value="Deactivation Date"/>
0223	<AttributeValue type="DateTime" value="\$NOW+31536000"/>
0224	</Attribute>
0225	</ResponsePayload>
0226	</BatchItem>
0227	</ResponseMessage>
	# TIME 5
0228	<RequestMessage>
0229	<RequestHeader>
0230	<ProtocolVersion>
0231	<ProtocolVersionMajor type="Integer" value="1"/>
0232	<ProtocolVersionMinor type="Integer" value="2"/>
0233	</ProtocolVersion>
0234	<BatchCount type="Integer" value="1"/>
0235	</RequestHeader>
0236	<BatchItem>
0237	<Operation type="Enumeration" value="Locate"/>
0238	<RequestPayload>
0239	<Attribute>
0240	<AttributeName type="TextString" value="Name"/>
0241	<AttributeValue>
0242	<NameValue type="TextString" value="TC-94-12-rekeyKey"/>
0243	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0244	</AttributeValue>
0245	</Attribute>

0246	</RequestPayload>
0247	</BatchItem>
0248	</RequestMessage>
0249	<ResponseMessage>
0250	<ResponseHeader>
0251	<ProtocolVersion>
0252	<ProtocolVersionMajor type="Integer" value="1"/>
0253	<ProtocolVersionMinor type="Integer" value="2"/>
0254	</ProtocolVersion>
0255	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0256	<BatchCount type="Integer" value="1"/>
0257	</ResponseHeader>
0258	<BatchItem>
0259	<Operation type="Enumeration" value="Locate"/>
0260	<ResultStatus type="Enumeration" value="Success"/>
0261	<ResponsePayload>
0262	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0263	</ResponsePayload>
0264	</BatchItem>
0265	</ResponseMessage>
# TIME 6	
0266	<RequestMessage>
0267	<RequestHeader>
0268	<ProtocolVersion>
0269	<ProtocolVersionMajor type="Integer" value="1"/>
0270	<ProtocolVersionMinor type="Integer" value="2"/>
0271	</ProtocolVersion>
0272	<BatchCount type="Integer" value="1"/>
0273	</RequestHeader>
0274	<BatchItem>
0275	<Operation type="Enumeration" value="Destroy"/>
0276	<RequestPayload>
0277	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0278	</RequestPayload>
0279	</BatchItem>
0280	</RequestMessage>
0281	<ResponseMessage>
0282	<ResponseHeader>
0283	<ProtocolVersion>
0284	<ProtocolVersionMajor type="Integer" value="1"/>
0285	<ProtocolVersionMinor type="Integer" value="2"/>
0286	</ProtocolVersion>
0287	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0288	<BatchCount type="Integer" value="1"/>
0289	</ResponseHeader>
0290	<BatchItem>
0291	<Operation type="Enumeration" value="Destroy"/>
0292	<ResultStatus type="Enumeration" value="Success"/>
0293	<ResponsePayload>
0294	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0295	</ResponsePayload>
0296	</BatchItem>
0297	</ResponseMessage>

0298 0299 0300 0301 0302 0303 0304 0305 0306 0307 0308 0309 0310 0311 0312 0313 0314 0315 0316 0317 0318 0319 0320 0321 0322 0323 0324	<pre># TIME 7 <RequestMessage> <RequestHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="2"/> </ProtocolVersion> <BatchOrderOption type="Boolean" value="true"/> <BatchCount type="Integer" value="2"/> </RequestHeader> <BatchItem> <Operation type="Enumeration" value="Revoke"/> <UniqueBatchItemID type="ByteString" value="64bf984d81eee045"/> <RequestPayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> <RevocationReason> <RevocationReasonCode type="Enumeration" value="CessationOfOperation"/> </RevocationReason> </RequestPayload> </BatchItem> <BatchItem> <Operation type="Enumeration" value="Destroy"/> <UniqueBatchItemID type="ByteString" value="6e140354775e324d"/> <RequestPayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> </RequestPayload> </BatchItem> </RequestMessage></pre>
0325 0326 0327 0328 0329 0330 0331 0332 0333 0334 0335 0336 0337 0338 0339 0340 0341 0342 0343 0344 0345 0346 0347 0348	<pre><ResponseMessage> <ResponseHeader> <ProtocolVersion> <ProtocolVersionMajor type="Integer" value="1"/> <ProtocolVersionMinor type="Integer" value="2"/> </ProtocolVersion> <TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/> <BatchCount type="Integer" value="2"/> </ResponseHeader> <BatchItem> <Operation type="Enumeration" value="Revoke"/> <UniqueBatchItemID type="ByteString" value="64bf984d81eee045"/> <ResultStatus type="Enumeration" value="Success"/> <ResponsePayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> </ResponsePayload> </BatchItem> <BatchItem> <Operation type="Enumeration" value="Destroy"/> <UniqueBatchItemID type="ByteString" value="6e140354775e324d"/> <ResultStatus type="Enumeration" value="Success"/> <ResponsePayload> <UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/> </ResponsePayload></pre>

0349	</BatchItem>
0350	</ResponseMessage>

858

859 2.3.18 TC-95-12 - Obtain Lease for Expired Key

860 Create a symmetric key with a specific name and obtain a lease. Revoke the key with state
861 'Compromised' and re-key the key. Try to obtain a lease on the old key which fails due to a
862 server policy which does not allow giving out leases for compromised keys. Locate the new key
863 with the original name. Get the new key and obtain a lease.

	# TIME 0
	# [Client-A]
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="TC-95-12-rekeyKey"/>
0030	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0031	</AttributeValue>
0032	</Attribute>
0033	<Attribute>
0034	<AttributeName type="TextString" value="Activation Date"/>
0035	<AttributeValue type="DateTime" value="\$NOW"/>
0036	</Attribute>
0037	</TemplateAttribute>
0038	</RequestPayload>

0039	</BatchItem>
0040	</RequestMessage>
0041	<ResponseMessage>
0042	<ResponseHeader>
0043	<ProtocolVersion>
0044	<ProtocolVersionMajor type="Integer" value="1"/>
0045	<ProtocolVersionMinor type="Integer" value="2"/>
0046	</ProtocolVersion>
0047	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0048	<BatchCount type="Integer" value="1"/>
0049	</ResponseHeader>
0050	<BatchItem>
0051	<Operation type="Enumeration" value="Create"/>
0052	<ResultStatus type="Enumeration" value="Success"/>
0053	<ResponsePayload>
0054	<ObjectType type="Enumeration" value="SymmetricKey"/>
0055	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0056	</ResponsePayload>
0057	</BatchItem>
0058	</ResponseMessage>
	# TIME 1
	# [Client-A]
0059	<RequestMessage>
0060	<RequestHeader>
0061	<ProtocolVersion>
0062	<ProtocolVersionMajor type="Integer" value="1"/>
0063	<ProtocolVersionMinor type="Integer" value="2"/>
0064	</ProtocolVersion>
0065	<BatchCount type="Integer" value="1"/>
0066	</RequestHeader>
0067	<BatchItem>
0068	<Operation type="Enumeration" value="Get"/>
0069	<RequestPayload>
0070	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0071	</RequestPayload>
0072	</BatchItem>
0073	</RequestMessage>
0074	<ResponseMessage>
0075	<ResponseHeader>
0076	<ProtocolVersion>
0077	<ProtocolVersionMajor type="Integer" value="1"/>
0078	<ProtocolVersionMinor type="Integer" value="2"/>
0079	</ProtocolVersion>
0080	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0081	<BatchCount type="Integer" value="1"/>
0082	</ResponseHeader>
0083	<BatchItem>
0084	<Operation type="Enumeration" value="Get"/>
0085	<ResultStatus type="Enumeration" value="Success"/>
0086	<ResponsePayload>
0087	<ObjectType type="Enumeration" value="SymmetricKey"/>
0088	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0089	<SymmetricKey>

0090	<KeyBlock>
0091	<KeyFormatType type="Enumeration" value="Raw"/>
0092	<KeyValue>
0093	<KeyMaterial type="ByteString"
	value="ef5a0e97a29b32034c66efbf26ad3e42"/>
0094	</KeyValue>
0095	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0096	<CryptographicLength type="Integer" value="128"/>
0097	</KeyBlock>
0098	</SymmetricKey>
0099	</ResponsePayload>
0100	</BatchItem>
0101	</ResponseMessage>
	# TIME 2
	# [Client-A]
0102	<RequestMessage>
0103	<RequestHeader>
0104	<ProtocolVersion>
0105	<ProtocolVersionMajor type="Integer" value="1"/>
0106	<ProtocolVersionMinor type="Integer" value="2"/>
0107	</ProtocolVersion>
0108	<BatchCount type="Integer" value="1"/>
0109	</RequestHeader>
0110	<BatchItem>
0111	<Operation type="Enumeration" value="ObtainLease"/>
0112	<RequestPayload>
0113	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0114	</RequestPayload>
0115	</BatchItem>
0116	</RequestMessage>
0117	<ResponseMessage>
0118	<ResponseHeader>
0119	<ProtocolVersion>
0120	<ProtocolVersionMajor type="Integer" value="1"/>
0121	<ProtocolVersionMinor type="Integer" value="2"/>
0122	</ProtocolVersion>
0123	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0124	<BatchCount type="Integer" value="1"/>
0125	</ResponseHeader>
0126	<BatchItem>
0127	<Operation type="Enumeration" value="ObtainLease"/>
0128	<ResultStatus type="Enumeration" value="Success"/>
0129	<ResponsePayload>
0130	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0131	<LeaseTime type="Interval" value="3600"/>
0132	<LastChangeDate type="DateTime" value="\$NOW"/>
0133	</ResponsePayload>
0134	</BatchItem>
0135	</ResponseMessage>
	# TIME 3
	# [Client-B]
0136	<RequestMessage>
0137	<RequestHeader>
0138	<ProtocolVersion>

0139	<ProtocolVersionMajor type="Integer" value="1"/>
0140	<ProtocolVersionMinor type="Integer" value="2"/>
0141	</ProtocolVersion>
0142	<BatchCount type="Integer" value="1"/>
0143	</RequestHeader>
0144	<BatchItem>
0145	<Operation type="Enumeration" value="Revoke"/>
0146	<RequestPayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0148	<RevocationReason>
0149	<RevocationReasonCode type="Enumeration"
	value="KeyCompromise"/>
0150	</RevocationReason>
0151	<CompromiseOccurrenceDate type="DateTime" value="\$NOW"/>
0152	</RequestPayload>
0153	</BatchItem>
0154	</RequestMessage>
0155	<ResponseMessage>
0156	<ResponseHeader>
0157	<ProtocolVersion>
0158	<ProtocolVersionMajor type="Integer" value="1"/>
0159	<ProtocolVersionMinor type="Integer" value="2"/>
0160	</ProtocolVersion>
0161	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0162	<BatchCount type="Integer" value="1"/>
0163	</ResponseHeader>
0164	<BatchItem>
0165	<Operation type="Enumeration" value="Revoke"/>
0166	<ResultStatus type="Enumeration" value="Success"/>
0167	<ResponsePayload>
0168	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0169	</ResponsePayload>
0170	</BatchItem>
0171	</ResponseMessage>
	# TIME 4
	# [Client-B]
0172	<RequestMessage>
0173	<RequestHeader>
0174	<ProtocolVersion>
0175	<ProtocolVersionMajor type="Integer" value="1"/>
0176	<ProtocolVersionMinor type="Integer" value="2"/>
0177	</ProtocolVersion>
0178	<BatchCount type="Integer" value="1"/>
0179	</RequestHeader>
0180	<BatchItem>
0181	<Operation type="Enumeration" value="ReKey"/>
0182	<RequestPayload>
0183	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0184	</RequestPayload>
0185	</BatchItem>
0186	</RequestMessage>
0187	<ResponseMessage>
0188	<ResponseHeader>

0189	<ProtocolVersion>
0190	<ProtocolVersionMajor type="Integer" value="1"/>
0191	<ProtocolVersionMinor type="Integer" value="2"/>
0192	</ProtocolVersion>
0193	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0194	<BatchCount type="Integer" value="1"/>
0195	</ResponseHeader>
0196	<BatchItem>
0197	<Operation type="Enumeration" value="ReKey"/>
0198	<ResultStatus type="Enumeration" value="Success"/>
0199	<ResponsePayload>
0200	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0201	</ResponsePayload>
0202	</BatchItem>
0203	</ResponseMessage>
	# TIME 5
	# [Client-A]
0204	<RequestMessage>
0205	<RequestHeader>
0206	<ProtocolVersion>
0207	<ProtocolVersionMajor type="Integer" value="1"/>
0208	<ProtocolVersionMinor type="Integer" value="2"/>
0209	</ProtocolVersion>
0210	<BatchCount type="Integer" value="1"/>
0211	</RequestHeader>
0212	<BatchItem>
0213	<Operation type="Enumeration" value="ObtainLease"/>
0214	<RequestPayload>
0215	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0216	</RequestPayload>
0217	</BatchItem>
0218	</RequestMessage>
0219	<ResponseMessage>
0220	<ResponseHeader>
0221	<ProtocolVersion>
0222	<ProtocolVersionMajor type="Integer" value="1"/>
0223	<ProtocolVersionMinor type="Integer" value="2"/>
0224	</ProtocolVersion>
0225	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0226	<BatchCount type="Integer" value="1"/>
0227	</ResponseHeader>
0228	<BatchItem>
0229	<Operation type="Enumeration" value="ObtainLease"/>
0230	<ResultStatus type="Enumeration" value="OperationFailed"/>
0231	<ResultReason type="Enumeration" value="PermissionDenied"/>
0232	<ResultMessage type="TextString" value="CO is in state
	Compromised, no lease given"/>
0233	</BatchItem>
0234	</ResponseMessage>
	# TIME 6
	# [Client-A]
0235	<RequestMessage>
0236	<RequestHeader>
0237	<ProtocolVersion>

0238	<ProtocolVersionMajor type="Integer" value="1"/>
0239	<ProtocolVersionMinor type="Integer" value="2"/>
0240	</ProtocolVersion>
0241	<BatchCount type="Integer" value="1"/>
0242	</RequestHeader>
0243	<BatchItem>
0244	<Operation type="Enumeration" value="Locate"/>
0245	<RequestPayload>
0246	<Attribute>
0247	<AttributeName type="TextString" value="Name"/>
0248	<AttributeValue>
0249	<NameValue type="TextString" value="TC-95-12-rekeyKey"/>
0250	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0251	</AttributeValue>
0252	</Attribute>
0253	</RequestPayload>
0254	</BatchItem>
0255	</RequestMessage>
0256	<ResponseMessage>
0257	<ResponseHeader>
0258	<ProtocolVersion>
0259	<ProtocolVersionMajor type="Integer" value="1"/>
0260	<ProtocolVersionMinor type="Integer" value="2"/>
0261	</ProtocolVersion>
0262	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0263	<BatchCount type="Integer" value="1"/>
0264	</ResponseHeader>
0265	<BatchItem>
0266	<Operation type="Enumeration" value="Locate"/>
0267	<ResultStatus type="Enumeration" value="Success"/>
0268	<ResponsePayload>
0269	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0270	</ResponsePayload>
0271	</BatchItem>
0272	</ResponseMessage>
	# TIME 7
	# [Client-A]
0273	<RequestMessage>
0274	<RequestHeader>
0275	<ProtocolVersion>
0276	<ProtocolVersionMajor type="Integer" value="1"/>
0277	<ProtocolVersionMinor type="Integer" value="2"/>
0278	</ProtocolVersion>
0279	<BatchCount type="Integer" value="1"/>
0280	</RequestHeader>
0281	<BatchItem>
0282	<Operation type="Enumeration" value="Get"/>
0283	<RequestPayload>
0284	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0285	</RequestPayload>
0286	</BatchItem>
0287	</RequestMessage>
0288	<ResponseMessage>

0289	<ResponseHeader>
0290	<ProtocolVersion>
0291	<ProtocolVersionMajor type="Integer" value="1"/>
0292	<ProtocolVersionMinor type="Integer" value="2"/>
0293	</ProtocolVersion>
0294	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0295	<BatchCount type="Integer" value="1"/>
0296	</ResponseHeader>
0297	<BatchItem>
0298	<Operation type="Enumeration" value="Get"/>
0299	<ResultStatus type="Enumeration" value="Success"/>
0300	<ResponsePayload>
0301	<ObjectType type="Enumeration" value="SymmetricKey"/>
0302	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0303	<SymmetricKey>
0304	<KeyBlock>
0305	<KeyFormatType type="Enumeration" value="Raw"/>
0306	<KeyValue>
0307	<KeyMaterial type="ByteString"
	value="525d4b0bbb66bcb538029d49a6f569a5"/>
0308	</KeyValue>
0309	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0310	<CryptographicLength type="Integer" value="128"/>
0311	</KeyBlock>
0312	</SymmetricKey>
0313	</ResponsePayload>
0314	</BatchItem>
0315	</ResponseMessage>
	# TIME 8
	# [Client-A]
0316	<RequestMessage>
0317	<RequestHeader>
0318	<ProtocolVersion>
0319	<ProtocolVersionMajor type="Integer" value="1"/>
0320	<ProtocolVersionMinor type="Integer" value="2"/>
0321	</ProtocolVersion>
0322	<BatchCount type="Integer" value="1"/>
0323	</RequestHeader>
0324	<BatchItem>
0325	<Operation type="Enumeration" value="ObtainLease"/>
0326	<RequestPayload>
0327	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0328	</RequestPayload>
0329	</BatchItem>
0330	</RequestMessage>
0331	<ResponseMessage>
0332	<ResponseHeader>
0333	<ProtocolVersion>
0334	<ProtocolVersionMajor type="Integer" value="1"/>
0335	<ProtocolVersionMinor type="Integer" value="2"/>
0336	</ProtocolVersion>
0337	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0338	<BatchCount type="Integer" value="1"/>
0339	</ResponseHeader>
0340	<BatchItem>

0341	<Operation type="Enumeration" value="ObtainLease"/>
0342	<ResultStatus type="Enumeration" value="Success"/>
0343	<ResponsePayload>
0344	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0345	<LeaseTime type="Interval" value="3600"/>
0346	<LastChangeDate type="DateTime" value="\$NOW"/>
0347	</ResponsePayload>
0348	</BatchItem>
0349	</ResponseMessage>
	# TIME 9
	# [Client-A]
0350	<RequestMessage>
0351	<RequestHeader>
0352	<ProtocolVersion>
0353	<ProtocolVersionMajor type="Integer" value="1"/>
0354	<ProtocolVersionMinor type="Integer" value="2"/>
0355	</ProtocolVersion>
0356	<BatchCount type="Integer" value="1"/>
0357	</RequestHeader>
0358	<BatchItem>
0359	<Operation type="Enumeration" value="Destroy"/>
0360	<RequestPayload>
0361	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0362	</RequestPayload>
0363	</BatchItem>
0364	</RequestMessage>
0365	<ResponseMessage>
0366	<ResponseHeader>
0367	<ProtocolVersion>
0368	<ProtocolVersionMajor type="Integer" value="1"/>
0369	<ProtocolVersionMinor type="Integer" value="2"/>
0370	</ProtocolVersion>
0371	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0372	<BatchCount type="Integer" value="1"/>
0373	</ResponseHeader>
0374	<BatchItem>
0375	<Operation type="Enumeration" value="Destroy"/>
0376	<ResultStatus type="Enumeration" value="Success"/>
0377	<ResponsePayload>
0378	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0379	</ResponsePayload>
0380	</BatchItem>
0381	</ResponseMessage>
	# TIME 10
	# [Client-A]
0382	<RequestMessage>
0383	<RequestHeader>
0384	<ProtocolVersion>
0385	<ProtocolVersionMajor type="Integer" value="1"/>
0386	<ProtocolVersionMinor type="Integer" value="2"/>
0387	</ProtocolVersion>
0388	<BatchOrderOption type="Boolean" value="true"/>
0389	<BatchCount type="Integer" value="2"/>

```

0390 </RequestHeader>
0391 <BatchItem>
0392   <Operation type="Enumeration" value="Revoke"/>
0393   <UniqueBatchItemID type="ByteString" value="e00004346ea64da4"/>
0394   <RequestPayload>
0395     <UniqueIdentifier type="TextString"
0396     value="$UNIQUE_IDENTIFIER_1"/>
0396     <RevocationReason>
0397       <RevocationReasonCode type="Enumeration"
0398       value="CessationOfOperation"/>
0398     </RevocationReason>
0399   </RequestPayload>
0400 </BatchItem>
0401 <BatchItem>
0402   <Operation type="Enumeration" value="Destroy"/>
0403   <UniqueBatchItemID type="ByteString" value="0376ca8cdcc8a2f1"/>
0404   <RequestPayload>
0405     <UniqueIdentifier type="TextString"
0406     value="$UNIQUE_IDENTIFIER_1"/>
0406   </RequestPayload>
0407 </BatchItem>
0408 </RequestMessage>
0409 <ResponseMessage>
0410   <ResponseHeader>
0411     <ProtocolVersion>
0412       <ProtocolVersionMajor type="Integer" value="1"/>
0413       <ProtocolVersionMinor type="Integer" value="2"/>
0414     </ProtocolVersion>
0415     <TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0416     <BatchCount type="Integer" value="2"/>
0417   </ResponseHeader>
0418   <BatchItem>
0419     <Operation type="Enumeration" value="Revoke"/>
0420     <UniqueBatchItemID type="ByteString" value="e00004346ea64da4"/>
0421     <ResultStatus type="Enumeration" value="Success"/>
0422     <ResponsePayload>
0423       <UniqueIdentifier type="TextString"
0424       value="$UNIQUE_IDENTIFIER_1"/>
0424     </ResponsePayload>
0425   </BatchItem>
0426   <BatchItem>
0427     <Operation type="Enumeration" value="Destroy"/>
0428     <UniqueBatchItemID type="ByteString" value="0376ca8cdcc8a2f1"/>
0429     <ResultStatus type="Enumeration" value="Success"/>
0430     <ResponsePayload>
0431       <UniqueIdentifier type="TextString"
0432       value="$UNIQUE_IDENTIFIER_1"/>
0432     </ResponsePayload>
0433   </BatchItem>
0434 </ResponseMessage>

```

864

865 2.3.19 TC-101-12 - Create a Key, Archive and Recover it

866 Create a symmetric key with a specified name, then use Locate to find the key and get the key.

867 Archive the key (asynchronous operation, use Poll until it completes) and use Get and Locate on

868 it, but both fail (Get returns an error and Locate returns no Unique Identifiers). Add the Storage
869 Status Mask to the Locate-command, indicating to the server to search in both online and
870 archived storage. The Locate then finds the archived key. Recover the key (asynchronous
871 operation, use Poll until it completes) from the archive, then repeat the Get operation which will
872 now succeed.

873 Since the client is unable to force the server to respond asynchronously, it is possible for a
874 server to respond synchronously to the requests issued at times 3 and 9, in which case the
875 expected responses are the ones shown at times 4 and 10 respectively.

876 Note: a server may perform Archive and Recover operations synchronously and not require the
877 use of Poll for the client to wait for the operation to complete

```
# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="2"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="Create"/>
0011     <RequestPayload>
0012       <ObjectType type="Enumeration" value="SymmetricKey"/>
0013       <TemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0016           <AttributeValue type="Enumeration" value="AES"/>
0017         </Attribute>
0018         <Attribute>
0019           <AttributeName type="TextString" value="Cryptographic
Length"/>
0020           <AttributeValue type="Integer" value="128"/>
0021         </Attribute>
0022         <Attribute>
0023           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0024           <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025         </Attribute>
0026         <Attribute>
0027           <AttributeName type="TextString" value="Name"/>
0028           <AttributeValue>
0029             <NameValue type="TextString" value="TC-101-12-
archiveKey"/>
0030             <NameType type="Enumeration"
value="UninterpretedTextString"/>
0031           </AttributeValue>
0032         </Attribute>
0033       </TemplateAttribute>
0034     </RequestPayload>
0035   </BatchItem>
```

0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="2"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
# TIME 1	
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="2"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="Locate"/>
0065	<RequestPayload>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Object Type"/>
0068	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Name"/>
0072	<AttributeValue>
0073	<NameValue type="TextString" value="TC-101-12-
	archiveKey"/>
0074	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0075	</AttributeValue>
0076	</Attribute>
0077	</RequestPayload>
0078	</BatchItem>
0079	</RequestMessage>
0080	<ResponseMessage>
0081	<ResponseHeader>
0082	<ProtocolVersion>
0083	<ProtocolVersionMajor type="Integer" value="1"/>
0084	<ProtocolVersionMinor type="Integer" value="2"/>
0085	</ProtocolVersion>
0086	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0087	<BatchCount type="Integer" value="1"/>

0088	</ResponseHeader>
0089	<BatchItem>
0090	<Operation type="Enumeration" value="Locate"/>
0091	<ResultStatus type="Enumeration" value="Success"/>
0092	<ResponsePayload>
0093	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0094	</ResponsePayload>
0095	</BatchItem>
0096	</ResponseMessage>
# TIME 2	
0097	<RequestMessage>
0098	<RequestHeader>
0099	<ProtocolVersion>
0100	<ProtocolVersionMajor type="Integer" value="1"/>
0101	<ProtocolVersionMinor type="Integer" value="2"/>
0102	</ProtocolVersion>
0103	<BatchCount type="Integer" value="1"/>
0104	</RequestHeader>
0105	<BatchItem>
0106	<Operation type="Enumeration" value="Get"/>
0107	<RequestPayload>
0108	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0109	</RequestPayload>
0110	</BatchItem>
0111	</RequestMessage>
0112	<ResponseMessage>
0113	<ResponseHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="2"/>
0117	</ProtocolVersion>
0118	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0119	<BatchCount type="Integer" value="1"/>
0120	</ResponseHeader>
0121	<BatchItem>
0122	<Operation type="Enumeration" value="Get"/>
0123	<ResultStatus type="Enumeration" value="Success"/>
0124	<ResponsePayload>
0125	<ObjectType type="Enumeration" value="SymmetricKey"/>
0126	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0127	<SymmetricKey>
0128	<KeyBlock>
0129	<KeyFormatType type="Enumeration" value="Raw"/>
0130	<KeyValue>
0131	<KeyMaterial type="ByteString"
	value="0b4c9fb659c5ce09ec12c3233d526f45"/>
0132	</KeyValue>
0133	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0134	<CryptographicLength type="Integer" value="128"/>
0135	</KeyBlock>
0136	</SymmetricKey>
0137	</ResponsePayload>
0138	</BatchItem>
0139	</ResponseMessage>

0140	# TIME 3
0141	<RequestMessage>
0142	<RequestHeader>
0143	<ProtocolVersion>
0144	<ProtocolVersionMajor type="Integer" value="1"/>
0145	<ProtocolVersionMinor type="Integer" value="2"/>
0146	</ProtocolVersion>
0147	<AsynchronousIndicator type="Boolean" value="true"/>
0148	<BatchCount type="Integer" value="1"/>
0149	</RequestHeader>
0150	<BatchItem>
0151	<Operation type="Enumeration" value="Archive"/>
0152	<RequestPayload>
0153	<UniqueIdentifier type="TextString"
0154	value="\$UNIQUE_IDENTIFIER_0"/>
0155	</RequestPayload>
0156	</BatchItem>
0157	</RequestMessage>
0158	<ResponseMessage>
0159	<ResponseHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="2"/>
0163	</ProtocolVersion>
0164	<TimeStamp type="DateTime" value="2012-04-27T08:14:28+00:00"/>
0165	<BatchCount type="Integer" value="1"/>
0166	</ResponseHeader>
0167	<BatchItem>
0168	<Operation type="Enumeration" value="Archive"/>
0169	<ResultStatus type="Enumeration" value="OperationPending"/>
0170	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
	</BatchItem>
	</ResponseMessage>
0171	# TIME 4
0172	# [REPEAT] until Archive response is returned
0173	<RequestMessage>
0174	<RequestHeader>
0175	<ProtocolVersion>
0176	<ProtocolVersionMajor type="Integer" value="1"/>
0177	<ProtocolVersionMinor type="Integer" value="2"/>
0178	</ProtocolVersion>
0179	<BatchCount type="Integer" value="1"/>
0180	</RequestHeader>
0181	<BatchItem>
0182	<Operation type="Enumeration" value="Poll"/>
0183	<RequestPayload>
0184	<AsynchronousCorrelationValue type="ByteString"
0185	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0186	</RequestPayload>
0187	</BatchItem>
0188	</RequestMessage>
0189	<ResponseMessage>
	<ResponseHeader>
	<ProtocolVersion>
	<ProtocolVersionMajor type="Integer" value="1"/>

0190	<ProtocolVersionMinor type="Integer" value="2"/>
0191	</ProtocolVersion>
0192	<TimeStamp type="DateTime" value="2012-04-27T08:14:30+00:00"/>
0193	<BatchCount type="Integer" value="1"/>
0194	</ResponseHeader>
0195	<BatchItem>
0196	<Operation type="Enumeration" value="Archive"/>
0197	<ResultStatus type="Enumeration" value="Success"/>
0198	<ResponsePayload>
0199	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0200	</ResponsePayload>
0201	</BatchItem>
0202	</ResponseMessage>
# TIME 5	
0203	<RequestMessage>
0204	<RequestHeader>
0205	<ProtocolVersion>
0206	<ProtocolVersionMajor type="Integer" value="1"/>
0207	<ProtocolVersionMinor type="Integer" value="2"/>
0208	</ProtocolVersion>
0209	<BatchCount type="Integer" value="1"/>
0210	</RequestHeader>
0211	<BatchItem>
0212	<Operation type="Enumeration" value="Get"/>
0213	<RequestPayload>
0214	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0215	</RequestPayload>
0216	</BatchItem>
0217	</RequestMessage>
0218	<ResponseMessage>
0219	<ResponseHeader>
0220	<ProtocolVersion>
0221	<ProtocolVersionMajor type="Integer" value="1"/>
0222	<ProtocolVersionMinor type="Integer" value="2"/>
0223	</ProtocolVersion>
0224	<TimeStamp type="DateTime" value="2012-04-27T08:14:32+00:00"/>
0225	<BatchCount type="Integer" value="1"/>
0226	</ResponseHeader>
0227	<BatchItem>
0228	<Operation type="Enumeration" value="Get"/>
0229	<ResultStatus type="Enumeration" value="OperationFailed"/>
0230	<ResultReason type="Enumeration" value="ObjectArchived"/>
0231	<ResultMessage type="TextString" value="Object is archived"/>
0232	</BatchItem>
0233	</ResponseMessage>
# TIME 6	
0234	<RequestMessage>
0235	<RequestHeader>
0236	<ProtocolVersion>
0237	<ProtocolVersionMajor type="Integer" value="1"/>
0238	<ProtocolVersionMinor type="Integer" value="2"/>
0239	</ProtocolVersion>
0240	<BatchCount type="Integer" value="1"/>
0241	</RequestHeader>

0242	<BatchItem>
0243	<Operation type="Enumeration" value="GetAttributes"/>
0244	<RequestPayload>
0245	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0246	<AttributeName type="TextString" value="Archive Date"/>
0247	</RequestPayload>
0248	</BatchItem>
0249	</RequestMessage>
0250	<ResponseMessage>
0251	<ResponseHeader>
0252	<ProtocolVersion>
0253	<ProtocolVersionMajor type="Integer" value="1"/>
0254	<ProtocolVersionMinor type="Integer" value="2"/>
0255	</ProtocolVersion>
0256	<TimeStamp type="DateTime" value="2012-04-27T08:14:32+00:00"/>
0257	<BatchCount type="Integer" value="1"/>
0258	</ResponseHeader>
0259	<BatchItem>
0260	<Operation type="Enumeration" value="GetAttributes"/>
0261	<ResultStatus type="Enumeration" value="Success"/>
0262	<ResponsePayload>
0263	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0264	<Attribute>
0265	<AttributeName type="TextString" value="Archive Date"/>
0266	<AttributeValue type="DateTime" value="2012-04-
	27T08:14:30+00:00"/>
0267	</Attribute>
0268	</ResponsePayload>
0269	</BatchItem>
0270	</ResponseMessage>
	# TIME 7
0271	<RequestMessage>
0272	<RequestHeader>
0273	<ProtocolVersion>
0274	<ProtocolVersionMajor type="Integer" value="1"/>
0275	<ProtocolVersionMinor type="Integer" value="2"/>
0276	</ProtocolVersion>
0277	<BatchCount type="Integer" value="1"/>
0278	</RequestHeader>
0279	<BatchItem>
0280	<Operation type="Enumeration" value="Locate"/>
0281	<RequestPayload>
0282	<Attribute>
0283	<AttributeName type="TextString" value="Object Type"/>
0284	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0285	</Attribute>
0286	<Attribute>
0287	<AttributeName type="TextString" value="Name"/>
0288	<AttributeValue>
0289	<NameValue type="TextString" value="TC-101-12-
	archiveKey"/>
0290	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0291	</AttributeValue>
0292	</Attribute>

0293	</RequestPayload>
0294	</BatchItem>
0295	</RequestMessage>
0296	<ResponseMessage>
0297	<ResponseHeader>
0298	<ProtocolVersion>
0299	<ProtocolVersionMajor type="Integer" value="1"/>
0300	<ProtocolVersionMinor type="Integer" value="2"/>
0301	</ProtocolVersion>
0302	<TimeStamp type="DateTime" value="2012-04-27T08:14:33+00:00"/>
0303	<BatchCount type="Integer" value="1"/>
0304	</ResponseHeader>
0305	<BatchItem>
0306	<Operation type="Enumeration" value="Locate"/>
0307	<ResultStatus type="Enumeration" value="Success"/>
0308	<ResponsePayload>
0309	</ResponsePayload>
0310	</BatchItem>
0311	</ResponseMessage>
# TIME 8	
0312	<RequestMessage>
0313	<RequestHeader>
0314	<ProtocolVersion>
0315	<ProtocolVersionMajor type="Integer" value="1"/>
0316	<ProtocolVersionMinor type="Integer" value="2"/>
0317	</ProtocolVersion>
0318	<BatchCount type="Integer" value="1"/>
0319	</RequestHeader>
0320	<BatchItem>
0321	<Operation type="Enumeration" value="Locate"/>
0322	<RequestPayload>
0323	<StorageStatusMask type="Integer" value="ArchivalStorage OnLineStorage"/>
0324	<Attribute>
0325	<AttributeName type="TextString" value="Object Type"/>
0326	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0327	</Attribute>
0328	<Attribute>
0329	<AttributeName type="TextString" value="Name"/>
0330	<AttributeValue>
0331	<NameValue type="TextString" value="TC-101-12- archiveKey"/>
0332	<NameType type="Enumeration" value="UninterpretedTextString"/>
0333	</AttributeValue>
0334	</Attribute>
0335	</RequestPayload>
0336	</BatchItem>
0337	</RequestMessage>
0338	<ResponseMessage>
0339	<ResponseHeader>
0340	<ProtocolVersion>
0341	<ProtocolVersionMajor type="Integer" value="1"/>
0342	<ProtocolVersionMinor type="Integer" value="2"/>
0343	</ProtocolVersion>
0344	<TimeStamp type="DateTime" value="2012-04-27T08:14:33+00:00"/>

0345	<BatchCount type="Integer" value="1"/>
0346	</ResponseHeader>
0347	<BatchItem>
0348	<Operation type="Enumeration" value="Locate"/>
0349	<ResultStatus type="Enumeration" value="Success"/>
0350	<ResponsePayload>
0351	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0352	</ResponsePayload>
0353	</BatchItem>
0354	</ResponseMessage>
# TIME 9	
0355	<RequestMessage>
0356	<RequestHeader>
0357	<ProtocolVersion>
0358	<ProtocolVersionMajor type="Integer" value="1"/>
0359	<ProtocolVersionMinor type="Integer" value="2"/>
0360	</ProtocolVersion>
0361	<AsynchronousIndicator type="Boolean" value="true"/>
0362	<BatchCount type="Integer" value="1"/>
0363	</RequestHeader>
0364	<BatchItem>
0365	<Operation type="Enumeration" value="Recover"/>
0366	<RequestPayload>
0367	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0368	</RequestPayload>
0369	</BatchItem>
0370	</RequestMessage>
0371	<ResponseMessage>
0372	<ResponseHeader>
0373	<ProtocolVersion>
0374	<ProtocolVersionMajor type="Integer" value="1"/>
0375	<ProtocolVersionMinor type="Integer" value="2"/>
0376	</ProtocolVersion>
0377	<TimeStamp type="DateTime" value="2012-04-27T08:14:33+00:00"/>
0378	<BatchCount type="Integer" value="1"/>
0379	</ResponseHeader>
0380	<BatchItem>
0381	<Operation type="Enumeration" value="Recover"/>
0382	<ResultStatus type="Enumeration" value="OperationPending"/>
0383	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0384	</BatchItem>
0385	</ResponseMessage>
# TIME 10	
# [REPEAT] until Recover response is returned	
0386	<RequestMessage>
0387	<RequestHeader>
0388	<ProtocolVersion>
0389	<ProtocolVersionMajor type="Integer" value="1"/>
0390	<ProtocolVersionMinor type="Integer" value="2"/>
0391	</ProtocolVersion>
0392	<BatchCount type="Integer" value="1"/>
0393	</RequestHeader>
0394	<BatchItem>

0395	<Operation type="Enumeration" value="Poll"/>
0396	<RequestPayload>
0397	<AsynchronousCorrelationValue type="ByteString"
	value="\$ASYNCHRONOUS_CORRELATION_VALUE"/>
0398	</RequestPayload>
0399	</BatchItem>
0400	</RequestMessage>
0401	<ResponseMessage>
0402	<ResponseHeader>
0403	<ProtocolVersion>
0404	<ProtocolVersionMajor type="Integer" value="1"/>
0405	<ProtocolVersionMinor type="Integer" value="2"/>
0406	</ProtocolVersion>
0407	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0408	<BatchCount type="Integer" value="1"/>
0409	</ResponseHeader>
0410	<BatchItem>
0411	<Operation type="Enumeration" value="Recover"/>
0412	<ResultStatus type="Enumeration" value="Success"/>
0413	<ResponsePayload>
0414	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0415	</ResponsePayload>
0416	</BatchItem>
0417	</ResponseMessage>
	# TIME 11
0418	<RequestMessage>
0419	<RequestHeader>
0420	<ProtocolVersion>
0421	<ProtocolVersionMajor type="Integer" value="1"/>
0422	<ProtocolVersionMinor type="Integer" value="2"/>
0423	</ProtocolVersion>
0424	<BatchCount type="Integer" value="1"/>
0425	</RequestHeader>
0426	<BatchItem>
0427	<Operation type="Enumeration" value="Get"/>
0428	<RequestPayload>
0429	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0430	</RequestPayload>
0431	</BatchItem>
0432	</RequestMessage>
0433	<ResponseMessage>
0434	<ResponseHeader>
0435	<ProtocolVersion>
0436	<ProtocolVersionMajor type="Integer" value="1"/>
0437	<ProtocolVersionMinor type="Integer" value="2"/>
0438	</ProtocolVersion>
0439	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0440	<BatchCount type="Integer" value="1"/>
0441	</ResponseHeader>
0442	<BatchItem>
0443	<Operation type="Enumeration" value="Get"/>
0444	<ResultStatus type="Enumeration" value="Success"/>
0445	<ResponsePayload>
0446	<ObjectType type="Enumeration" value="SymmetricKey"/>

0447	<UniqueIdentifier type="TextString"
0448	value="\$UNIQUE_IDENTIFIER_0"/>
0449	<SymmetricKey>
0450	<KeyBlock>
0451	<KeyFormatType type="Enumeration" value="Raw"/>
0452	<KeyValue>
0453	<KeyMaterial type="ByteString"
0454	value="0b4c9fb659c5ce09ec12c3233d526f45"/>
0455	</KeyValue>
0456	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0457	<CryptographicLength type="Integer" value="128"/>
0458	</KeyBlock>
0459	</SymmetricKey>
0460	</ResponsePayload>
0461	</BatchItem>
0462	</ResponseMessage>
0463	# TIME 12
0464	<RequestMessage>
0465	<RequestHeader>
0466	<ProtocolVersion>
0467	<ProtocolVersionMajor type="Integer" value="1"/>
0468	<ProtocolVersionMinor type="Integer" value="2"/>
0469	</ProtocolVersion>
0470	<BatchCount type="Integer" value="1"/>
0471	</RequestHeader>
0472	<BatchItem>
0473	<Operation type="Enumeration" value="Destroy"/>
0474	<RequestPayload>
0475	<UniqueIdentifier type="TextString"
0476	value="\$UNIQUE_IDENTIFIER_0"/>
0477	</RequestPayload>
0478	</BatchItem>
0479	</RequestMessage>
0480	<ResponseMessage>
0481	<ResponseHeader>
0482	<ProtocolVersion>
0483	<ProtocolVersionMajor type="Integer" value="1"/>
0484	<ProtocolVersionMinor type="Integer" value="2"/>
0485	</ProtocolVersion>
0486	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0487	<BatchCount type="Integer" value="1"/>
0488	</ResponseHeader>
0489	<BatchItem>
0490	<Operation type="Enumeration" value="Destroy"/>
0491	<ResultStatus type="Enumeration" value="Success"/>
0492	<ResponsePayload>
0493	<UniqueIdentifier type="TextString"
0494	value="\$UNIQUE_IDENTIFIER_0"/>
0495	</ResponsePayload>
0496	</BatchItem>
0497	</ResponseMessage>

878

879 2.3.20 TC-111-12 - Credential, Operation Policy, Destroy Date

880 Pass a Credential object of type Username and Password in the message header in all requests
881 for identification purposes. Create a symmetric key and set the Operation Policy Name attribute
882 to 'default'. Using another Username and Password Credential, attempt to perform a Get
883 operation batched with a Get Attribute List on the created symmetric key - according to the
884 Default Operation Policy, both these request SHALL fail, and with the Batch Error Continuation
885 Option set to 'Continue', the client SHALL also receive both response payloads. Using the first
886 (correct) Credential, Destroy the object and then get the Destroy Date attribute.

887 The message exchanges shown in this test case assume that the first Credential (Fred) is valid
888 and the second credential (Barney) is either invalid or does not have access to the newly created
889 key (which should always be true under the 'default' Operation Policy).

890 Note: a server can elect to not return meta-data for destroyed objects and in those
891 circumstances the Get Attributes operation may fail.

```
# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="2"/>
0006     </ProtocolVersion>
0007     <Authentication>
0008       <Credential>
0009         <CredentialType type="Enumeration"
value="UsernameAndPassword"/>
0010         <CredentialValue>
0011           <Username type="TextString" value="Fred"/>
0012           <Password type="TextString" value="password1"/>
0013         </CredentialValue>
0014       </Credential>
0015     </Authentication>
0016     <BatchCount type="Integer" value="1"/>
0017   </RequestHeader>
0018   <BatchItem>
0019     <Operation type="Enumeration" value="Create"/>
0020     <RequestPayload>
0021       <ObjectType type="Enumeration" value="SymmetricKey"/>
0022       <TemplateAttribute>
0023         <Attribute>
0024           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0025           <AttributeValue type="Enumeration" value="AES"/>
0026         </Attribute>
0027         <Attribute>
0028           <AttributeName type="TextString" value="Cryptographic
Length"/>
0029           <AttributeValue type="Integer" value="128"/>
0030         </Attribute>
0031         <Attribute>
0032           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
```

0033	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0034	</Attribute>
0035	<Attribute>
0036	<AttributeName type="TextString" value="Name"/>
0037	<AttributeValue>
0038	<NameValue type="TextString" value="TC-111-12-key1"/>
0039	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0040	</AttributeValue>
0041	</Attribute>
0042	<Attribute>
0043	<AttributeName type="TextString" value="Operation Policy
	Name"/>
0044	<AttributeValue type="TextString" value="default"/>
0045	</Attribute>
0046	<Attribute>
0047	<AttributeName type="TextString" value="Cryptographic
	Parameters"/>
0048	<AttributeValue>
0049	<BlockCipherMode type="Enumeration" value="CBC"/>
0050	<PaddingMethod type="Enumeration" value="PKCS5"/>
0051	<HashingAlgorithm type="Enumeration" value="SHA_1"/>
0052	</AttributeValue>
0053	</Attribute>
0054	</TemplateAttribute>
0055	</RequestPayload>
0056	</BatchItem>
0057	</RequestMessage>
0058	<ResponseMessage>
0059	<ResponseHeader>
0060	<ProtocolVersion>
0061	<ProtocolVersionMajor type="Integer" value="1"/>
0062	<ProtocolVersionMinor type="Integer" value="2"/>
0063	</ProtocolVersion>
0064	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0065	<BatchCount type="Integer" value="1"/>
0066	</ResponseHeader>
0067	<BatchItem>
0068	<Operation type="Enumeration" value="Create"/>
0069	<ResultStatus type="Enumeration" value="Success"/>
0070	<ResponsePayload>
0071	<ObjectType type="Enumeration" value="SymmetricKey"/>
0072	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0073	</ResponsePayload>
0074	</BatchItem>
0075	</ResponseMessage>
	# TIME 1
0076	<RequestMessage>
0077	<RequestHeader>
0078	<ProtocolVersion>
0079	<ProtocolVersionMajor type="Integer" value="1"/>
0080	<ProtocolVersionMinor type="Integer" value="2"/>
0081	</ProtocolVersion>
0082	<Authentication>
0083	<Credential>
0084	<CredentialType type="Enumeration"

0085	value="UsernameAndPassword"/>
0086	<CredentialValue>
0087	<Username type="TextString" value="Fred"/>
0088	<Password type="TextString" value="password1"/>
0089	</CredentialValue>
0090	</Credential>
0091	</Authentication>
0092	<BatchCount type="Integer" value="2"/>
0093	</RequestHeader>
0094	<BatchItem>
0095	<Operation type="Enumeration" value="GetAttributes"/>
0096	<UniqueBatchItemID type="ByteString" value="55d88770e2556dab"/>
0097	<RequestPayload>
0098	<UniqueIdentifier type="TextString"
0099	value="\$UNIQUE_IDENTIFIER_0"/>
0100	<AttributeName type="TextString" value="Operation Policy
0101	Name"/>
0102	</RequestPayload>
0103	</BatchItem>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Get"/>
0106	<UniqueBatchItemID type="ByteString" value="eb864ee01f1f98cd"/>
0107	<RequestPayload>
0108	<UniqueIdentifier type="TextString"
0109	value="\$UNIQUE_IDENTIFIER_0"/>
0110	</RequestPayload>
0111	</BatchItem>
0112	</RequestMessage>
0113	<ResponseMessage>
0114	<ResponseHeader>
0115	<ProtocolVersion>
0116	<ProtocolVersionMajor type="Integer" value="1"/>
0117	<ProtocolVersionMinor type="Integer" value="2"/>
0118	</ProtocolVersion>
0119	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0120	<BatchCount type="Integer" value="2"/>
0121	</ResponseHeader>
0122	<BatchItem>
0123	<Operation type="Enumeration" value="GetAttributes"/>
0124	<UniqueBatchItemID type="ByteString" value="55d88770e2556dab"/>
0125	<ResultStatus type="Enumeration" value="Success"/>
0126	<ResponsePayload>
0127	<UniqueIdentifier type="TextString"
0128	value="\$UNIQUE_IDENTIFIER_0"/>
0129	<Attribute>
0130	<AttributeName type="TextString" value="Operation Policy
0131	Name"/>
0132	<AttributeValue type="TextString" value="default"/>
0133	</Attribute>
0134	</ResponsePayload>
0135	</BatchItem>
	<BatchItem>
	<Operation type="Enumeration" value="Get"/>
	<UniqueBatchItemID type="ByteString" value="eb864ee01f1f98cd"/>
	<ResultStatus type="Enumeration" value="Success"/>
	<ResponsePayload>
	<ObjectType type="Enumeration" value="SymmetricKey"/>

0136	<UniqueIdentifier type="TextString"
0137	value="\$UNIQUE_IDENTIFIER_0"/>
0138	<SymmetricKey>
0139	<KeyBlock>
0140	<KeyFormatType type="Enumeration" value="Raw"/>
0141	<KeyValue>
0142	<KeyMaterial type="ByteString"
0143	value="30e55f4b230b34ce8afc476c66f8351b"/>
0144	</KeyValue>
0145	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0146	<CryptographicLength type="Integer" value="128"/>
0147	</KeyBlock>
0148	</SymmetricKey>
0149	</ResponsePayload>
0150	</BatchItem>
0151	</ResponseMessage>
0152	# TIME 2
0153	<RequestMessage>
0154	<RequestHeader>
0155	<ProtocolVersion>
0156	<ProtocolVersionMajor type="Integer" value="1"/>
0157	<ProtocolVersionMinor type="Integer" value="2"/>
0158	</ProtocolVersion>
0159	<Authentication>
0160	<Credential>
0161	<CredentialType type="Enumeration"
0162	value="UsernameAndPassword"/>
0163	<CredentialValue>
0164	<Username type="TextString" value="Barney"/>
0165	<Password type="TextString" value="secret2"/>
0166	</CredentialValue>
0167	</Credential>
0168	</Authentication>
0169	<BatchErrorContinuationOption type="Enumeration"
0170	value="Continue"/>
0171	<BatchOrderOption type="Boolean" value="true"/>
0172	<BatchCount type="Integer" value="2"/>
0173	</RequestHeader>
0174	<BatchItem>
0175	<Operation type="Enumeration" value="Get"/>
0176	<UniqueBatchItemID type="ByteString" value="4f0e6d3dba3d0495"/>
0177	<RequestPayload>
0178	<UniqueIdentifier type="TextString"
0179	value="\$UNIQUE_IDENTIFIER_0"/>
0180	</RequestPayload>
0181	</BatchItem>
0182	<BatchItem>
0183	<Operation type="Enumeration" value="GetAttributeList"/>
0184	<UniqueBatchItemID type="ByteString" value="9b937e7cd50b233b"/>
0185	<RequestPayload>
0186	<UniqueIdentifier type="TextString"
0187	value="\$UNIQUE_IDENTIFIER_0"/>
0188	</RequestPayload>
0189	</BatchItem>
0190	</RequestMessage>
0191	<ResponseMessage>
0192	<ResponseHeader>

0186	<ProtocolVersion>
0187	<ProtocolVersionMajor type="Integer" value="1"/>
0188	<ProtocolVersionMinor type="Integer" value="2"/>
0189	</ProtocolVersion>
0190	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0191	<BatchCount type="Integer" value="2"/>
0192	</ResponseHeader>
0193	<BatchItem>
0194	<Operation type="Enumeration" value="Get"/>
0195	<UniqueBatchItemID type="ByteString" value="4f0e6d3dba3d0495"/>
0196	<ResultStatus type="Enumeration" value="OperationFailed"/>
0197	<ResultReason type="Enumeration" value="PermissionDenied"/>
0198	<ResultMessage type="TextString" value="Access denied"/>
0199	</BatchItem>
0200	<BatchItem>
0201	<Operation type="Enumeration" value="GetAttributeList"/>
0202	<UniqueBatchItemID type="ByteString" value="9b937e7cd50b233b"/>
0203	<ResultStatus type="Enumeration" value="OperationFailed"/>
0204	<ResultReason type="Enumeration" value="PermissionDenied"/>
0205	<ResultMessage type="TextString" value="Access denied"/>
0206	</BatchItem>
0207	</ResponseMessage>
# TIME 3	
0208	<RequestMessage>
0209	<RequestHeader>
0210	<ProtocolVersion>
0211	<ProtocolVersionMajor type="Integer" value="1"/>
0212	<ProtocolVersionMinor type="Integer" value="2"/>
0213	</ProtocolVersion>
0214	<Authentication>
0215	<Credential>
0216	<CredentialType type="Enumeration"
	value="UsernameAndPassword"/>
0217	<CredentialValue>
0218	<Username type="TextString" value="Fred"/>
0219	<Password type="TextString" value="password1"/>
0220	</CredentialValue>
0221	</Credential>
0222	</Authentication>
0223	<BatchCount type="Integer" value="1"/>
0224	</RequestHeader>
0225	<BatchItem>
0226	<Operation type="Enumeration" value="Destroy"/>
0227	<RequestPayload>
0228	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0229	</RequestPayload>
0230	</BatchItem>
0231	</RequestMessage>
0232	<ResponseMessage>
0233	<ResponseHeader>
0234	<ProtocolVersion>
0235	<ProtocolVersionMajor type="Integer" value="1"/>
0236	<ProtocolVersionMinor type="Integer" value="2"/>
0237	</ProtocolVersion>
0238	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0239	<BatchCount type="Integer" value="1"/>

0240	</ResponseHeader>
0241	<BatchItem>
0242	<Operation type="Enumeration" value="Destroy"/>
0243	<ResultStatus type="Enumeration" value="Success"/>
0244	<ResponsePayload>
0245	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0246	</ResponsePayload>
0247	</BatchItem>
0248	</ResponseMessage>
# TIME 4	
0249	<RequestMessage>
0250	<RequestHeader>
0251	<ProtocolVersion>
0252	<ProtocolVersionMajor type="Integer" value="1"/>
0253	<ProtocolVersionMinor type="Integer" value="2"/>
0254	</ProtocolVersion>
0255	<Authentication>
0256	<Credential>
0257	<CredentialType type="Enumeration"
	value="UsernameAndPassword"/>
0258	<CredentialValue>
0259	<Username type="TextString" value="Fred"/>
0260	<Password type="TextString" value="password1"/>
0261	</CredentialValue>
0262	</Credential>
0263	</Authentication>
0264	<BatchCount type="Integer" value="1"/>
0265	</RequestHeader>
0266	<BatchItem>
0267	<Operation type="Enumeration" value="GetAttributes"/>
0268	<RequestPayload>
0269	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0270	<AttributeName type="TextString" value="Destroy Date"/>
0271	</RequestPayload>
0272	</BatchItem>
0273	</RequestMessage>
0274	<ResponseMessage>
0275	<ResponseHeader>
0276	<ProtocolVersion>
0277	<ProtocolVersionMajor type="Integer" value="1"/>
0278	<ProtocolVersionMinor type="Integer" value="2"/>
0279	</ProtocolVersion>
0280	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0281	<BatchCount type="Integer" value="1"/>
0282	</ResponseHeader>
0283	<BatchItem>
0284	<Operation type="Enumeration" value="GetAttributes"/>
0285	<ResultStatus type="Enumeration" value="Success"/>
0286	<ResponsePayload>
0287	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0288	<Attribute>
0289	<AttributeName type="TextString" value="Destroy Date"/>
0290	<AttributeValue type="DateTime" value="2012-04-
	27T08:14:35+00:00"/>

0291	</Attribute>
0292	</ResponsePayload>
0293	</BatchItem>
0294	</ResponseMessage>

892

893 2.3.21 TC-112-12 - Device Credential, Operation Policy, Destroy Date

894 Pass a Credential object of type Device Credential in the message header in all requests for
895 identification purposes. Create a symmetric key and set the Operation Policy Name attribute to
896 'default'. Using another Credential, attempt to perform a Get operation batched with a Get
897 Attribute List on the created symmetric key. According to the Default Operation Policy, both
898 these request SHALL fail, and with the Batch Error Continuation Option set to 'Continue', the
899 client SHALL also receive both response payloads. Using the first Credential, Destroy the object
900 and get the Destroy Date attribute. The message exchanges shown in this test case assume that
901 the first Credential (devID2233) is valid and the second credential (devID4444) is either invalid
902 or does not have access to the newly created key (which should always be true under the
903 'default' Operation Policy).

904 Note: a server can elect to not return meta-data for destroyed objects and in those
905 circumstances the Get Attributes operation may fail.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<Authentication>
0008	<Credential>
0009	<CredentialType type="Enumeration" value="Device"/>
0010	<CredentialValue>
0011	<DeviceSerialNumber type="TextString"
	value="serNum123456"/>
0012	<Password type="TextString" value="secret"/>
0013	<DeviceIdentifier type="TextString" value="devID2233"/>
0014	<NetworkIdentifier type="TextString" value="netID9000"/>
0015	<MachineIdentifier type="TextString" value="machineID1"/>
0016	<MediaIdentifier type="TextString" value="mediaID313"/>
0017	</CredentialValue>
0018	</Credential>
0019	</Authentication>
0020	<BatchCount type="Integer" value="1"/>
0021	</RequestHeader>
0022	<BatchItem>
0023	<Operation type="Enumeration" value="Create"/>
0024	<RequestPayload>
0025	<ObjectType type="Enumeration" value="SymmetricKey"/>
0026	<TemplateAttribute>
0027	<Attribute>
0028	<AttributeName type="TextString" value="Cryptographic"
	Algorithm"/>

0029	<AttributeValue type="Enumeration" value="AES"/>
0030	</Attribute>
0031	<Attribute>
0032	<AttributeName type="TextString" value="Cryptographic Length"/>
0033	<AttributeValue type="Integer" value="128"/>
0034	</Attribute>
0035	<Attribute>
0036	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0037	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0038	</Attribute>
0039	<Attribute>
0040	<AttributeName type="TextString" value="Name"/>
0041	<AttributeValue>
0042	<NameValue type="TextString" value="TC-112-12-key1"/>
0043	<NameType type="Enumeration" value="UninterpretedTextString"/>
0044	</AttributeValue>
0045	</Attribute>
0046	<Attribute>
0047	<AttributeName type="TextString" value="Operation Policy Name"/>
0048	<AttributeValue type="TextString" value="default"/>
0049	</Attribute>
0050	<Attribute>
0051	<AttributeName type="TextString" value="Cryptographic Parameters"/>
0052	<AttributeValue>
0053	<BlockCipherMode type="Enumeration" value="CBC"/>
0054	<PaddingMethod type="Enumeration" value="PKCS5"/>
0055	<HashingAlgorithm type="Enumeration" value="SHA_1"/>
0056	</AttributeValue>
0057	</Attribute>
0058	</TemplateAttribute>
0059	</RequestPayload>
0060	</BatchItem>
0061	</RequestMessage>
0062	<ResponseMessage>
0063	<ResponseHeader>
0064	<ProtocolVersion>
0065	<ProtocolVersionMajor type="Integer" value="1"/>
0066	<ProtocolVersionMinor type="Integer" value="2"/>
0067	</ProtocolVersion>
0068	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0069	<BatchCount type="Integer" value="1"/>
0070	</ResponseHeader>
0071	<BatchItem>
0072	<Operation type="Enumeration" value="Create"/>
0073	<ResultStatus type="Enumeration" value="Success"/>
0074	<ResponsePayload>
0075	<ObjectType type="Enumeration" value="SymmetricKey"/>
0076	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0077	</ResponsePayload>
0078	</BatchItem>
0079	</ResponseMessage>

	# TIME 1
0080	<RequestMessage>
0081	<RequestHeader>
0082	<ProtocolVersion>
0083	<ProtocolVersionMajor type="Integer" value="1"/>
0084	<ProtocolVersionMinor type="Integer" value="2"/>
0085	</ProtocolVersion>
0086	<Authentication>
0087	<Credential>
0088	<CredentialType type="Enumeration" value="Device"/>
0089	<CredentialValue>
0090	<DeviceSerialNumber type="TextString"
	value="serNum123456"/>
0091	<Password type="TextString" value="secret"/>
0092	<DeviceIdentifier type="TextString" value="devID2233"/>
0093	<NetworkIdentifier type="TextString" value="netID9000"/>
0094	<MachineIdentifier type="TextString" value="machineID1"/>
0095	<MediaIdentifier type="TextString" value="mediaID313"/>
0096	</CredentialValue>
0097	</Credential>
0098	</Authentication>
0099	<BatchCount type="Integer" value="2"/>
0100	</RequestHeader>
0101	<BatchItem>
0102	<Operation type="Enumeration" value="GetAttributes"/>
0103	<UniqueBatchItemID type="ByteString" value="e705e27dc0ba7789"/>
0104	<RequestPayload>
0105	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0106	<AttributeName type="TextString" value="Operation Policy
	Name"/>
0107	</RequestPayload>
0108	</BatchItem>
0109	<BatchItem>
0110	<Operation type="Enumeration" value="Get"/>
0111	<UniqueBatchItemID type="ByteString" value="50a7f741a1119826"/>
0112	<RequestPayload>
0113	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0114	</RequestPayload>
0115	</BatchItem>
0116	</RequestMessage>
0117	<ResponseMessage>
0118	<ResponseHeader>
0119	<ProtocolVersion>
0120	<ProtocolVersionMajor type="Integer" value="1"/>
0121	<ProtocolVersionMinor type="Integer" value="2"/>
0122	</ProtocolVersion>
0123	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0124	<BatchCount type="Integer" value="2"/>
0125	</ResponseHeader>
0126	<BatchItem>
0127	<Operation type="Enumeration" value="GetAttributes"/>
0128	<UniqueBatchItemID type="ByteString" value="e705e27dc0ba7789"/>
0129	<ResultStatus type="Enumeration" value="Success"/>
0130	<ResponsePayload>
0131	<UniqueIdentifier type="TextString"

0132	value="\$UNIQUE_IDENTIFIER_0"/>
0133	<Attribute>
0133	<AttributeName type="TextString" value="Operation Policy
0134	Name"/>
0134	<AttributeValue type="TextString" value="default"/>
0135	</Attribute>
0136	</ResponsePayload>
0137	</BatchItem>
0138	<BatchItem>
0139	<Operation type="Enumeration" value="Get"/>
0140	<UniqueBatchItemID type="ByteString" value="50a7f741a1119826"/>
0141	<ResultStatus type="Enumeration" value="Success"/>
0142	<ResponsePayload>
0143	<ObjectType type="Enumeration" value="SymmetricKey"/>
0144	<UniqueIdentifier type="TextString"
0145	value="\$UNIQUE_IDENTIFIER_0"/>
0145	<SymmetricKey>
0146	<KeyBlock>
0147	<KeyFormatType type="Enumeration" value="Raw"/>
0148	<KeyValue>
0149	<KeyMaterial type="ByteString"
0150	value="acfeaffdbdd17d0e63624a22083ee4b6"/>
0151	</KeyValue>
0151	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0152	<CryptographicLength type="Integer" value="128"/>
0153	</KeyBlock>
0154	</SymmetricKey>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
# TIME 2	
0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="2"/>
0163	</ProtocolVersion>
0164	<Authentication>
0165	<Credential>
0166	<CredentialType type="Enumeration" value="Device"/>
0167	<CredentialValue>
0168	<DeviceSerialNumber type="TextString"
0169	value="serNum101010"/>
0170	<Password type="TextString" value="passwd"/>
0171	<DeviceIdentifier type="TextString" value="devID4444"/>
0171	<NetworkIdentifier type="TextString" value="netID9"/>
0172	<MachineIdentifier type="TextString"
0173	value="machineID1111"/>
0174	<MediaIdentifier type="TextString" value="mediaID0000"/>
0175	</CredentialValue>
0176	</Credential>
0177	</Authentication>
0177	<BatchErrorContinuationOption type="Enumeration"
0178	value="Continue"/>
0178	<BatchOrderOption type="Boolean" value="true"/>
0179	<BatchCount type="Integer" value="2"/>
0180	</RequestHeader>

0181	<BatchItem>
0182	<Operation type="Enumeration" value="Get"/>
0183	<UniqueBatchItemID type="ByteString" value="1154049d742c498e"/>
0184	<RequestPayload>
0185	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0186	</RequestPayload>
0187	</BatchItem>
0188	<BatchItem>
0189	<Operation type="Enumeration" value="GetAttributeList"/>
0190	<UniqueBatchItemID type="ByteString" value="8ae55c6e91d97b05"/>
0191	<RequestPayload>
0192	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0193	</RequestPayload>
0194	</BatchItem>
0195	</RequestMessage>
0196	<ResponseMessage>
0197	<ResponseHeader>
0198	<ProtocolVersion>
0199	<ProtocolVersionMajor type="Integer" value="1"/>
0200	<ProtocolVersionMinor type="Integer" value="2"/>
0201	</ProtocolVersion>
0202	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0203	<BatchCount type="Integer" value="2"/>
0204	</ResponseHeader>
0205	<BatchItem>
0206	<Operation type="Enumeration" value="Get"/>
0207	<UniqueBatchItemID type="ByteString" value="1154049d742c498e"/>
0208	<ResultStatus type="Enumeration" value="OperationFailed"/>
0209	<ResultReason type="Enumeration" value="PermissionDenied"/>
0210	<ResultMessage type="TextString" value="Access denied"/>
0211	</BatchItem>
0212	<BatchItem>
0213	<Operation type="Enumeration" value="GetAttributeList"/>
0214	<UniqueBatchItemID type="ByteString" value="8ae55c6e91d97b05"/>
0215	<ResultStatus type="Enumeration" value="OperationFailed"/>
0216	<ResultReason type="Enumeration" value="PermissionDenied"/>
0217	<ResultMessage type="TextString" value="Access denied"/>
0218	</BatchItem>
0219	</ResponseMessage>
	# TIME 3
0220	<RequestMessage>
0221	<RequestHeader>
0222	<ProtocolVersion>
0223	<ProtocolVersionMajor type="Integer" value="1"/>
0224	<ProtocolVersionMinor type="Integer" value="2"/>
0225	</ProtocolVersion>
0226	<Authentication>
0227	<Credential>
0228	<CredentialType type="Enumeration" value="Device"/>
0229	<CredentialValue>
0230	<DeviceSerialNumber type="TextString"
	value="serNum123456"/>
0231	<Password type="TextString" value="secret"/>
0232	<DeviceIdentifier type="TextString" value="devID2233"/>
0233	<NetworkIdentifier type="TextString" value="netID9000"/>

0234	<MachineIdentifier type="TextString" value="machineID1"/>
0235	<MediaIdentifier type="TextString" value="mediaID313"/>
0236	</CredentialValue>
0237	</Credential>
0238	</Authentication>
0239	<BatchCount type="Integer" value="1"/>
0240	</RequestHeader>
0241	<BatchItem>
0242	<Operation type="Enumeration" value="Destroy"/>
0243	<RequestPayload>
0244	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0245	</RequestPayload>
0246	</BatchItem>
0247	</RequestMessage>
0248	<ResponseMessage>
0249	<ResponseHeader>
0250	<ProtocolVersion>
0251	<ProtocolVersionMajor type="Integer" value="1"/>
0252	<ProtocolVersionMinor type="Integer" value="2"/>
0253	</ProtocolVersion>
0254	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0255	<BatchCount type="Integer" value="1"/>
0256	</ResponseHeader>
0257	<BatchItem>
0258	<Operation type="Enumeration" value="Destroy"/>
0259	<ResultStatus type="Enumeration" value="Success"/>
0260	<ResponsePayload>
0261	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0262	</ResponsePayload>
0263	</BatchItem>
0264	</ResponseMessage>
	# TIME 4
0265	<RequestMessage>
0266	<RequestHeader>
0267	<ProtocolVersion>
0268	<ProtocolVersionMajor type="Integer" value="1"/>
0269	<ProtocolVersionMinor type="Integer" value="2"/>
0270	</ProtocolVersion>
0271	<Authentication>
0272	<Credential>
0273	<CredentialType type="Enumeration" value="Device"/>
0274	<CredentialValue>
0275	<DeviceSerialNumber type="TextString"
	value="serNum123456"/>
0276	<Password type="TextString" value="secret"/>
0277	<DeviceIdentifier type="TextString" value="devID2233"/>
0278	<NetworkIdentifier type="TextString" value="netID9000"/>
0279	<MachineIdentifier type="TextString" value="machineID1"/>
0280	<MediaIdentifier type="TextString" value="mediaID313"/>
0281	</CredentialValue>
0282	</Credential>
0283	</Authentication>
0284	<BatchCount type="Integer" value="1"/>
0285	</RequestHeader>
0286	<BatchItem>

0287	<Operation type="Enumeration" value="GetAttributes"/>
0288	<RequestPayload>
0289	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0290	<AttributeName type="TextString" value="Destroy Date"/>
0291	</RequestPayload>
0292	</BatchItem>
0293	</RequestMessage>
0294	<ResponseMessage>
0295	<ResponseHeader>
0296	<ProtocolVersion>
0297	<ProtocolVersionMajor type="Integer" value="1"/>
0298	<ProtocolVersionMinor type="Integer" value="2"/>
0299	</ProtocolVersion>
0300	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0301	<BatchCount type="Integer" value="1"/>
0302	</ResponseHeader>
0303	<BatchItem>
0304	<Operation type="Enumeration" value="GetAttributes"/>
0305	<ResultStatus type="Enumeration" value="Success"/>
0306	<ResponsePayload>
0307	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0308	<Attribute>
0309	<AttributeName type="TextString" value="Destroy Date"/>
0310	<AttributeValue type="DateTime" value="2012-04-
	27T08:14:35+00:00"/>
0311	</Attribute>
0312	</ResponsePayload>
0313	</BatchItem>
0314	</ResponseMessage>

906

907 2.3.22 TC-121-12 - Query, Maximum Response Size

908 Perform a Query operation, querying the Operations and Objects supported by the server, with
909 a restriction on the Maximum Response Size set in the request header. Since the resulting Query
910 response is too large, an error is returned. Increase the Maximum Response Size, resubmit the
911 Query request, and get a successful response.

912 Note: the list of object types supported and operations will vary depending on the server
913 implementation. The server can report the Vendor Identification in whatever TextString form
914 the vendor selects. The server may return vendor specific tags in the Server Information
915 structure indicating additional vendor-specific information about the server.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<MaximumResponseSize type="Integer" value="256"/>
0008	<BatchCount type="Integer" value="1"/>

0009	</RequestHeader>
0010	<BatchItem>
0011	<Operation type="Enumeration" value="Query"/>
0012	<RequestPayload>
0013	<QueryFunction type="Enumeration" value="QueryOperations"/>
0014	<QueryFunction type="Enumeration" value="QueryObjects"/>
0015	</RequestPayload>
0016	</BatchItem>
0017	</RequestMessage>
0018	<ResponseMessage>
0019	<ResponseHeader>
0020	<ProtocolVersion>
0021	<ProtocolVersionMajor type="Integer" value="1"/>
0022	<ProtocolVersionMinor type="Integer" value="2"/>
0023	</ProtocolVersion>
0024	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0025	<BatchCount type="Integer" value="1"/>
0026	</ResponseHeader>
0027	<BatchItem>
0028	<Operation type="Enumeration" value="Query"/>
0029	<ResultStatus type="Enumeration" value="OperationFailed"/>
0030	<ResultReason type="Enumeration" value="ResponseTooLarge"/>
0031	<ResultMessage type="TextString" value="Response size: 648, Maximum Response Size indicated in request: 256"/>
0032	</BatchItem>
0033	</ResponseMessage>
0034	# TIME 1
0035	<RequestMessage>
0036	<RequestHeader>
0037	<ProtocolVersion>
0038	<ProtocolVersionMajor type="Integer" value="1"/>
0039	<ProtocolVersionMinor type="Integer" value="2"/>
0040	</ProtocolVersion>
0041	<MaximumResponseSize type="Integer" value="2048"/>
0042	<BatchCount type="Integer" value="1"/>
0043	</RequestHeader>
0044	<BatchItem>
0045	<Operation type="Enumeration" value="Query"/>
0046	<RequestPayload>
0047	<QueryFunction type="Enumeration" value="QueryOperations"/>
0048	<QueryFunction type="Enumeration" value="QueryObjects"/>
0049	<QueryFunction type="Enumeration" value="QueryServerInformation"/>
0050	</RequestPayload>
0051	</BatchItem>
0052	</RequestMessage>
0053	<ResponseMessage>
0054	<ResponseHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="2"/>
0058	</ProtocolVersion>
0059	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0060	<BatchCount type="Integer" value="1"/>
0061	</ResponseHeader>
0062	<BatchItem>

0062	<Operation type="Enumeration" value="Query"/>
0063	<ResultStatus type="Enumeration" value="Success"/>
0064	<ResponsePayload>
0065	<Operation type="Enumeration" value="Query"/>
0066	<Operation type="Enumeration" value="Locate"/>
0067	<Operation type="Enumeration" value="Destroy"/>
0068	<Operation type="Enumeration" value="Get"/>
0069	<Operation type="Enumeration" value="Create"/>
0070	<Operation type="Enumeration" value="Register"/>
0071	<Operation type="Enumeration" value="GetAttributes"/>
0072	<Operation type="Enumeration" value="GetAttributeList"/>
0073	<Operation type="Enumeration" value="AddAttribute"/>
0074	<Operation type="Enumeration" value="ModifyAttribute"/>
0075	<Operation type="Enumeration" value="DeleteAttribute"/>
0076	<Operation type="Enumeration" value="Activate"/>
0077	<Operation type="Enumeration" value="Revoke"/>
0078	<Operation type="Enumeration" value="Poll"/>
0079	<Operation type="Enumeration" value="Cancel"/>
0080	<Operation type="Enumeration" value="Check"/>
0081	<Operation type="Enumeration" value="GetUsageAllocation"/>
0082	<Operation type="Enumeration" value="CreateKeyPair"/>
0083	<Operation type="Enumeration" value="ReKey"/>
0084	<Operation type="Enumeration" value="Archive"/>
0085	<Operation type="Enumeration" value="Recover"/>
0086	<Operation type="Enumeration" value="ObtainLease"/>
0087	<Operation type="Enumeration" value="ReKeyKeyPair"/>
0088	<Operation type="Enumeration" value="Certify"/>
0089	<Operation type="Enumeration" value="ReCertify"/>
0090	<Operation type="Enumeration" value="DiscoverVersions"/>
0091	<Operation type="Enumeration" value="Notify"/>
0092	<Operation type="Enumeration" value="Put"/>
0093	<Operation type="Enumeration" value="RNGRetrieve"/>
0094	<Operation type="Enumeration" value="RNGSeed"/>
0095	<Operation type="Enumeration" value="Encrypt"/>
0096	<Operation type="Enumeration" value="Decrypt"/>
0097	<Operation type="Enumeration" value="Sign"/>
0098	<Operation type="Enumeration" value="SignatureVerify"/>
0099	<Operation type="Enumeration" value="MAC"/>
0100	<Operation type="Enumeration" value="MACVerify"/>
0101	<Operation type="Enumeration" value="Hash"/>
0102	<Operation type="Enumeration" value="CreateSplitKey"/>
0103	<Operation type="Enumeration" value="JoinSplitKey"/>
0104	<ObjectType type="Enumeration" value="Certificate"/>
0105	<ObjectType type="Enumeration" value="SymmetricKey"/>
0106	<ObjectType type="Enumeration" value="SecretData"/>
0107	<ObjectType type="Enumeration" value="PublicKey"/>
0108	<ObjectType type="Enumeration" value="PrivateKey"/>
0109	<ObjectType type="Enumeration" value="Template"/>
0110	<ObjectType type="Enumeration" value="OpaqueObject"/>
0111	<ObjectType type="Enumeration" value="SplitKey"/>
0112	<ObjectType type="Enumeration" value="PGPKey"/>
0113	<VendorIdentification type="TextString" value="SOME-VENDOR-NAME"/>
0114	<ServerInformation>
0115	</ServerInformation>
0116	</ResponsePayload>
0117	</BatchItem>

0118	</ResponseMessage>
------	--------------------

916

917 2.3.23 TC-122-12 - Query Vendor Extensions

918 Query the server for a list and map of vendor extension tags it recognizes.

919 Note: Extension Type is an Integer as there is no corresponding enumerated type for the Item
920 Type field.

921

0001	# TIME 0
0002	<RequestMessage>
0003	<RequestHeader>
0004	<ProtocolVersion>
0005	<ProtocolVersionMajor type="Integer" value="1"/>
0006	<ProtocolVersionMinor type="Integer" value="2"/>
0007	</ProtocolVersion>
0008	<BatchCount type="Integer" value="1"/>
0009	</BatchCount>
0010	<Operation type="Enumeration" value="Query"/>
0011	<RequestPayload>
0012	<QueryFunction type="Enumeration" value="QueryExtensionList"/>
0013	</QueryFunction>
0014	</BatchItem>
0015	</RequestMessage>
0016	<ResponseMessage>
0017	<ResponseHeader>
0018	<ProtocolVersion>
0019	<ProtocolVersionMajor type="Integer" value="1"/>
0020	<ProtocolVersionMinor type="Integer" value="2"/>
0021	</ProtocolVersion>
0022	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0023	<BatchCount type="Integer" value="1"/>
0024	</BatchCount>
0025	<Operation type="Enumeration" value="Query"/>
0026	<ResultStatus type="Enumeration" value="Success"/>
0027	<ResponsePayload>
0028	<ExtensionInformation>
0029	<ExtensionName type="TextString" value="ACME LOCATION"/>
0030	</ExtensionName>
0031	<ExtensionInformation>
0032	<ExtensionName type="TextString" value="ACME ZIP CODE"/>
0033	</ExtensionName>
0034	</ResponsePayload>
0035	</BatchItem>
0036	</ResponseMessage>
0037	
0038	# TIME 1
0039	<RequestMessage>
0040	<RequestHeader>
0041	<ProtocolVersion>
0042	<ProtocolVersionMajor type="Integer" value="1"/>
0043	<ProtocolVersionMinor type="Integer" value="2"/>

0043	</ProtocolVersion>
0044	<BatchCount type="Integer" value="1"/>
0045	</RequestHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Query"/>
0048	<RequestPayload>
0049	<QueryFunction type="Enumeration" value="QueryExtensionMap"/>
0050	</RequestPayload>
0051	</BatchItem>
0052	</RequestMessage>
0053	<ResponseMessage>
0054	<ResponseHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="2"/>
0058	</ProtocolVersion>
0059	<TimeStamp type="DateTime" value="2012-04-27T08:14:35+00:00"/>
0060	<BatchCount type="Integer" value="1"/>
0061	</ResponseHeader>
0062	<BatchItem>
0063	<Operation type="Enumeration" value="Query"/>
0064	<ResultStatus type="Enumeration" value="Success"/>
0065	<ResponsePayload>
0066	<ExtensionInformation>
0067	<ExtensionName type="TextString" value="ACME LOCATION"/>
0068	<ExtensionTag type="Integer" value="5548545"/>
0069	<ExtensionType type="Integer" value="7"/>
0070	</ExtensionInformation>
0071	<ExtensionInformation>
0072	<ExtensionName type="TextString" value="ACME ZIP CODE"/>
0073	<ExtensionTag type="Integer" value="5548546"/>
0074	<ExtensionType type="Integer" value="2"/>
0075	</ExtensionInformation>
0076	</ResponsePayload>
0077	</BatchItem>
0078	</ResponseMessage>

922

923 2.3.24 TC-131-12 - Register an Asymmetric Key Pair in PKCS1 Format

924 Register a private key in the PKCS_1 key format, then register the corresponding public key, also
925 in PKCS_1 format, with the Link attribute pointing to the previously registered private key.
926 Thereafter add the Link attribute to the private key, and perform Locate operations to find the
927 public and private keys using the Link attribute. Get both the private and public keys in PKCS_1
928 key format, then destroy both the private and the public key.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>

```
0009 <BatchItem>
0010   <Operation type="Enumeration" value="Register"/>
0011   <RequestPayload>
0012     <ObjectType type="Enumeration" value="PrivateKey"/>
0013     <TemplateAttribute>
0014       <Attribute>
0015         <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0016         <AttributeValue type="Integer" value="Sign"/>
0017       </Attribute>
0018     </Attribute>
0019     <AttributeName type="TextString" value="x-ID"/>
0020     <AttributeValue type="TextString" value="TC-131-12-
prikey1"/>
0021   </Attribute>
0022 </TemplateAttribute>
0023 <PrivateKey>
0024   <KeyBlock>
0025     <KeyFormatType type="Enumeration" value="PKCS_1"/>
0026     <KeyValue>
0027       <KeyMaterial type="ByteString"
value="308204a50201000282010100ab7f161c0042496ccd6c6d4dad9199734353
57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483
46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa
2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650
89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c
795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f
91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281
5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050
203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a
7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f
a74cde5fdafabdb6aa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b
2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0
e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a
a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e
3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78
965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8
c3cdc2464744a793713dafb9f1dbc799ff96423fecdc3ba794286bce920f4b5c183f
99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967
4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c
ec4a00d4d4db41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064
b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e
59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4
990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766
b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab
7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0
e94ad1ee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db
e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa
elebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2
7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eae922fd75d5b16b1a5
61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bfff1a85a72
6a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171
666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520
a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a
1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d34941
7e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f812
9c32341a8b44f"/>
```

0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0030	<CryptographicLength type="Integer" value="2048"/>
0031	</KeyBlock>
0032	</PrivateKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="2"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="2"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PublicKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0068	<AttributeValue type="Integer" value="Verify"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>
0073	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0075	</AttributeValue>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-131-12-
	pubkey1"/>

0080	</Attribute>
0081	</TemplateAttribute>
0082	<PublicKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString"
	value="3082010a0282010100ab7f161c0042496ccd6c6d4dad9199734353577760
	03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b
	8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89
	b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981
	35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328
	abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013
	da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612
	a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010
	001"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0089	<CryptographicLength type="Integer" value="2048"/>
0090	</KeyBlock>
0091	</PublicKey>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="2"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0109	</ResponsePayload>
0110	</BatchItem>
0111	</ResponseMessage>
	# TIME 2
0112	<RequestMessage>
0113	<RequestHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="2"/>
0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="AddAttribute"/>
0122	<RequestPayload>
0123	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>

0125	<AttributeName type="TextString" value="Link"/>
0126	<AttributeValue>
0127	<LinkType type="Enumeration" value="PublicKeyLink"/>
0128	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0129	</AttributeValue>
0130	</Attribute>
0131	</RequestPayload>
0132	</BatchItem>
0133	</RequestMessage>
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="2"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="AddAttribute"/>
0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0148	<Attribute>
0149	<AttributeName type="TextString" value="Link"/>
0150	<AttributeValue>
0151	<LinkType type="Enumeration" value="PublicKeyLink"/>
0152	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0153	</AttributeValue>
0154	</Attribute>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
	# TIME 3
0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="2"/>
0163	</ProtocolVersion>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Locate"/>
0168	<RequestPayload>
0169	<Attribute>
0170	<AttributeName type="TextString" value="Object Type"/>
0171	<AttributeValue type="Enumeration" value="PublicKey"/>
0172	</Attribute>
0173	<Attribute>
0174	<AttributeName type="TextString" value="Link"/>
0175	<AttributeValue>
0176	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0177	<LinkedObjectIdentifier type="TextString"

0178	value="\$UNIQUE_IDENTIFIER_0"/>
0179	</AttributeValue>
0180	</Attribute>
0181	</RequestPayload>
0182	</BatchItem>
0183	</RequestMessage>
0183	<ResponseMessage>
0184	<ResponseHeader>
0185	<ProtocolVersion>
0186	<ProtocolVersionMajor type="Integer" value="1"/>
0187	<ProtocolVersionMinor type="Integer" value="2"/>
0188	</ProtocolVersion>
0189	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0190	<BatchCount type="Integer" value="1"/>
0191	</ResponseHeader>
0192	<BatchItem>
0193	<Operation type="Enumeration" value="Locate"/>
0194	<ResultStatus type="Enumeration" value="Success"/>
0195	<ResponsePayload>
0196	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0197	</ResponsePayload>
0198	</BatchItem>
0199	</ResponseMessage>
0200	# TIME 4
0200	<RequestMessage>
0201	<RequestHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="2"/>
0205	</ProtocolVersion>
0206	<BatchCount type="Integer" value="1"/>
0207	</RequestHeader>
0208	<BatchItem>
0209	<Operation type="Enumeration" value="Locate"/>
0210	<RequestPayload>
0211	<Attribute>
0212	<AttributeName type="TextString" value="Object Type"/>
0213	<AttributeValue type="Enumeration" value="PrivateKey"/>
0214	</Attribute>
0215	<Attribute>
0216	<AttributeName type="TextString" value="Link"/>
0217	<AttributeValue>
0218	<LinkType type="Enumeration" value="PublicKeyLink"/>
0219	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0220	</AttributeValue>
0221	</Attribute>
0222	</RequestPayload>
0223	</BatchItem>
0224	</RequestMessage>
0225	<ResponseMessage>
0226	<ResponseHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="2"/>

0230	</ProtocolVersion>
0231	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0232	<BatchCount type="Integer" value="1"/>
0233	</ResponseHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="Locate"/>
0236	<ResultStatus type="Enumeration" value="Success"/>
0237	<ResponsePayload>
0238	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0239	</ResponsePayload>
0240	</BatchItem>
0241	</ResponseMessage>
# TIME 5	
0242	<RequestMessage>
0243	<RequestHeader>
0244	<ProtocolVersion>
0245	<ProtocolVersionMajor type="Integer" value="1"/>
0246	<ProtocolVersionMinor type="Integer" value="2"/>
0247	</ProtocolVersion>
0248	<BatchCount type="Integer" value="1"/>
0249	</RequestHeader>
0250	<BatchItem>
0251	<Operation type="Enumeration" value="Get"/>
0252	<RequestPayload>
0253	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0254	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0255	</RequestPayload>
0256	</BatchItem>
0257	</RequestMessage>
0258	<ResponseMessage>
0259	<ResponseHeader>
0260	<ProtocolVersion>
0261	<ProtocolVersionMajor type="Integer" value="1"/>
0262	<ProtocolVersionMinor type="Integer" value="2"/>
0263	</ProtocolVersion>
0264	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0265	<BatchCount type="Integer" value="1"/>
0266	</ResponseHeader>
0267	<BatchItem>
0268	<Operation type="Enumeration" value="Get"/>
0269	<ResultStatus type="Enumeration" value="Success"/>
0270	<ResponsePayload>
0271	<ObjectType type="Enumeration" value="PrivateKey"/>
0272	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0273	<PrivateKey>
0274	<KeyBlock>
0275	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0276	<KeyValue>
0277	<KeyMaterial type="ByteString"
	value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353
	57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483
	46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa
	2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650
	89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c

	795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618fa74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0aa49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8c3cdc2464744a793713dafb9f1dbc799ff96423fec3cba794286bce920f4b5c183f99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fbl1d5659674c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04cec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0e94adlee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920dbe22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aae1ebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee27d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eaeafa922fd75d5b16b1a561fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a726a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d349417e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f8129c32341a8b44f"/>
0278	</KeyValue>
0279	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0280	<CryptographicLength type="Integer" value="2048"/>
0281	</KeyBlock>
0282	</PrivateKey>
0283	</ResponsePayload>
0284	</BatchItem>
0285	</ResponseMessage>
	# TIME 6
0286	<RequestMessage>
0287	<RequestHeader>
0288	<ProtocolVersion>
0289	<ProtocolVersionMajor type="Integer" value="1"/>
0290	<ProtocolVersionMinor type="Integer" value="2"/>
0291	</ProtocolVersion>
0292	<BatchCount type="Integer" value="1"/>
0293	</RequestHeader>
0294	<BatchItem>
0295	<Operation type="Enumeration" value="Get"/>
0296	<RequestPayload>
0297	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0298	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0299	</RequestPayload>
0300	</BatchItem>
0301	</RequestMessage>

0302	<ResponseMessage>
0303	<ResponseHeader>
0304	<ProtocolVersion>
0305	<ProtocolVersionMajor type="Integer" value="1"/>
0306	<ProtocolVersionMinor type="Integer" value="2"/>
0307	</ProtocolVersion>
0308	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0309	<BatchCount type="Integer" value="1"/>
0310	</ResponseHeader>
0311	<BatchItem>
0312	<Operation type="Enumeration" value="Get"/>
0313	<ResultStatus type="Enumeration" value="Success"/>
0314	<ResponsePayload>
0315	<ObjectType type="Enumeration" value="PublicKey"/>
0316	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0317	<PublicKey>
0318	<KeyBlock>
0319	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0320	<KeyValue>
0321	<KeyMaterial type="ByteString"
	value="3082010a0282010100ab7f161c0042496ccd6c6d4dadb9199734353577760
	03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b
	8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89
	b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981
	35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328
	abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013
	da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612
	a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010
	001"/>
0322	</KeyValue>
0323	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0324	<CryptographicLength type="Integer" value="2048"/>
0325	</KeyBlock>
0326	</PublicKey>
0327	</ResponsePayload>
0328	</BatchItem>
0329	</ResponseMessage>
	# TIME 7
0330	<RequestMessage>
0331	<RequestHeader>
0332	<ProtocolVersion>
0333	<ProtocolVersionMajor type="Integer" value="1"/>
0334	<ProtocolVersionMinor type="Integer" value="2"/>
0335	</ProtocolVersion>
0336	<BatchCount type="Integer" value="1"/>
0337	</RequestHeader>
0338	<BatchItem>
0339	<Operation type="Enumeration" value="Destroy"/>
0340	<RequestPayload>
0341	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0342	</RequestPayload>
0343	</BatchItem>
0344	</RequestMessage>
0345	<ResponseMessage>
0346	<ResponseHeader>

0347	<ProtocolVersion>
0348	<ProtocolVersionMajor type="Integer" value="1"/>
0349	<ProtocolVersionMinor type="Integer" value="2"/>
0350	</ProtocolVersion>
0351	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0352	<BatchCount type="Integer" value="1"/>
0353	</ResponseHeader>
0354	<BatchItem>
0355	<Operation type="Enumeration" value="Destroy"/>
0356	<ResultStatus type="Enumeration" value="Success"/>
0357	<ResponsePayload>
0358	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0359	</ResponsePayload>
0360	</BatchItem>
0361	</ResponseMessage>
# TIME 8	
0362	<RequestMessage>
0363	<RequestHeader>
0364	<ProtocolVersion>
0365	<ProtocolVersionMajor type="Integer" value="1"/>
0366	<ProtocolVersionMinor type="Integer" value="2"/>
0367	</ProtocolVersion>
0368	<BatchCount type="Integer" value="1"/>
0369	</RequestHeader>
0370	<BatchItem>
0371	<Operation type="Enumeration" value="Destroy"/>
0372	<RequestPayload>
0373	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0374	</RequestPayload>
0375	</BatchItem>
0376	</RequestMessage>
0377	<ResponseMessage>
0378	<ResponseHeader>
0379	<ProtocolVersion>
0380	<ProtocolVersionMajor type="Integer" value="1"/>
0381	<ProtocolVersionMinor type="Integer" value="2"/>
0382	</ProtocolVersion>
0383	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0384	<BatchCount type="Integer" value="1"/>
0385	</ResponseHeader>
0386	<BatchItem>
0387	<Operation type="Enumeration" value="Destroy"/>
0388	<ResultStatus type="Enumeration" value="Success"/>
0389	<ResponsePayload>
0390	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0391	</ResponsePayload>
0392	</BatchItem>
0393	</ResponseMessage>

930 2.3.25 TC-132-12 - Register an Asymmetric Key Pair and a Corresponding 931 X509 Certificate

- 932 Register a public/private key pair in the PKCS_1 key format and a corresponding X509 certificate.
933 Add the appropriate links between the registered objects. Make sure the certificate was
934 registered and the attributes set correctly by listing and retrieving the attributes. Get the keys
935 and certificate, and finally destroy all the registered objects.

```

# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="2"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="Register"/>
0011     <RequestPayload>
0012       <ObjectType type="Enumeration" value="PublicKey"/>
0013       <TemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0016           <AttributeValue type="Integer" value="Verify"/>
0017         </Attribute>
0018         <Attribute>
0019           <AttributeName type="TextString" value="x-ID"/>
0020           <AttributeValue type="TextString" value="TC-132-12-
pubkey1"/>
0021         </Attribute>
0022       </TemplateAttribute>
0023       <PublicKey>
0024         <KeyBlock>
0025           <KeyFormatType type="Enumeration" value="PKCS_1"/>
0026           <KeyValue>
0027             <KeyMaterial type="ByteString"
value="3082010a0282010100ab7f161c0042496ccd6c6d4dadb9199734353577760
03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b
8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89
b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981
35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328
abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013
da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612
a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010
001"/>
0028             </KeyValue>
0029           <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0030           <CryptographicLength type="Integer" value="2048"/>
0031         </KeyBlock>
0032       </PublicKey>
0033     </RequestPayload>
0034   </BatchItem>
0035 </RequestMessage>

```

0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="2"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="2"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PrivateKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0068	<AttributeValue type="Integer" value="Sign"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>
0073	<LinkType type="Enumeration" value="PublicKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0075	</AttributeValue>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-132-12-
	prikey1"/>
0080	</Attribute>
0081	</TemplateAttribute>
0082	<PrivateKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString"
	value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353

	57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618fa74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0aa49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8c3cdc2464744a793713dafb9f1dbcb799ff96423fecdd3cba794286bce920f4b5c183f99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d5659674c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04cec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab7877a6a868063e542a7186d431e8d27c19ac0414584033942e9fff6e2973bb7b2d8b0e94adlee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920dbe22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aaelebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee27d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eae9a922fd75d5b16b1a561fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a726a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d349417e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f8129c32341a8b44f"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0089	<CryptographicLength type="Integer" value="2048"/>
0090	</KeyBlock>
0091	</PrivateKey>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="2"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString"

0109	value="\$UNIQUE_IDENTIFIER_1"/>
0110	</ResponsePayload>
0111	</BatchItem>
0112	</ResponseMessage>
0112	# TIME 2
0113	<RequestMessage>
0114	<RequestHeader>
0115	<ProtocolVersion>
0116	<ProtocolVersionMajor type="Integer" value="1"/>
0117	<ProtocolVersionMinor type="Integer" value="2"/>
0118	</ProtocolVersion>
0119	<BatchCount type="Integer" value="1"/>
0120	</RequestHeader>
0121	<BatchItem>
0122	<Operation type="Enumeration" value="Register"/>
0123	<RequestPayload>
0124	<ObjectType type="Enumeration" value="Certificate"/>
0125	<TemplateAttribute>
0126	<Attribute>
0127	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0128	<AttributeValue type="Integer" value="Verify Sign"/>
0129	</Attribute>
0130	<Attribute>
0131	<AttributeName type="TextString" value="Link"/>
0132	<AttributeValue type="TextString" value="Link"/>
0133	<LinkType type="Enumeration" value="PublicKeyLink"/>
0134	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0135	</Attribute>
0136	<Attribute>
0137	<AttributeName type="TextString" value="x-ID"/>
0138	<AttributeValue type="TextString" value="TC-132-12-cert1"/>
0139	</Attribute>
0140	</TemplateAttribute>
0141	</Certificate>
0142	<CertificateType type="Enumeration" value="X_509"/>
0143	<CertificateValue type="ByteString" value="30820312308201faa003020102020101300d06092a864886f70d0101050500303b310b3009060355040613025553310d300b060355040a130454455354310e300c060355040b13054f41534953310d300b060355040313044b4d4950301e170d3130313130313233353935395a170d3230313130313233353935395a303b310b3009060355040613025553310d300b060355040a130454455354310e300c060355040b13054f41534953310d300b060355040313044b4d495030820122300d06092a864886f70d01010105000382010f003082010a0282010100ab7f161c0042496ccd6c6d4dadb919973435357776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89b9bee9e60ald7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010001a321301f301d0603551d0e0416041404e57bd2c431b2e816e180a19823fac858273f6b300d06092a864886f70d01010505000382010100a876adbc6c8e0ff017216e195fea76bfff61a567c9a13dc50d13fec12a4273c441547cfabcb5d61d99

0144	1e966319df72c0d41ba826a45112ff26089a2344f4d71cf7c921b4bdfaef1600d1ba
0145	aa15336057e014b8b496d4fae9e8a6c1da9aeb6cbc960cbf2fae77f587ec4bb28204
0146	5338845b88dd9aeaa53e482a36e734e4f5f03b9d0dfc4cafc6bb34ea9053e52bd609
0147	ee01e86d9b09fb51120c19834a997b09ce08d79e81311762f974bb1c8c09186c4d78
	933e0db38e905084877e147c78af52fae07192ff166d19fa94a11cc11b27ed050f7a
	27fae13b205a574c4ee00aa8bd65d0d7057c985c839ef336a441ed53a53c6b6b696f
	1bdeb5f7ea811ebb25a7f86"/>
	</Certificate>
	</RequestPayload>
	</BatchItem>
	</RequestMessage>
0148	<ResponseMessage>
0149	<ResponseHeader>
0150	<ProtocolVersion>
0151	<ProtocolVersionMajor type="Integer" value="1"/>
0152	<ProtocolVersionMinor type="Integer" value="2"/>
0153	</ProtocolVersion>
0154	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0155	<BatchCount type="Integer" value="1"/>
0156	</ResponseHeader>
0157	<BatchItem>
0158	<Operation type="Enumeration" value="Register"/>
0159	<ResultStatus type="Enumeration" value="Success"/>
0160	<ResponsePayload>
0161	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0162	</ResponsePayload>
0163	</BatchItem>
0164	</ResponseMessage>
0165	# TIME 3
0166	<RequestMessage>
0167	<RequestHeader>
0168	<ProtocolVersion>
0169	<ProtocolVersionMajor type="Integer" value="1"/>
0170	<ProtocolVersionMinor type="Integer" value="2"/>
0171	</ProtocolVersion>
0172	<BatchCount type="Integer" value="2"/>
0173	</RequestHeader>
0174	<BatchItem>
0175	<Operation type="Enumeration" value="AddAttribute"/>
0176	<UniqueBatchItemID type="ByteString" value="31f81bfb0f0492bd"/>
0177	<RequestPayload>
0178	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0179	<Attribute>
0180	<AttributeName type="TextString" value="Link"/>
0181	<AttributeValue>
0182	<LinkType type="Enumeration" value="PrivateKeyLink"/>
	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0183	</AttributeValue>
0184	</Attribute>
0185	</RequestPayload>
0186	</BatchItem>
0187	<BatchItem>
0188	<Operation type="Enumeration" value="AddAttribute"/>
0189	<UniqueBatchItemID type="ByteString" value="ba865701c7837be2"/>

0190	<RequestPayload>
0191	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0192	<Attribute>
0193	<AttributeName type="TextString" value="Link"/>
0194	<AttributeValue>
0195	<LinkType type="Enumeration" value="CertificateLink"/>
0196	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0197	</AttributeValue>
0198	</Attribute>
0199	</RequestPayload>
0200	</BatchItem>
0201	</RequestMessage>
0202	<ResponseMessage>
0203	<ResponseHeader>
0204	<ProtocolVersion>
0205	<ProtocolVersionMajor type="Integer" value="1"/>
0206	<ProtocolVersionMinor type="Integer" value="2"/>
0207	</ProtocolVersion>
0208	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0209	<BatchCount type="Integer" value="2"/>
0210	</ResponseHeader>
0211	<BatchItem>
0212	<Operation type="Enumeration" value="AddAttribute"/>
0213	<UniqueBatchItemID type="ByteString" value="31f81bfb0f0492bd"/>
0214	<ResultStatus type="Enumeration" value="Success"/>
0215	<ResponsePayload>
0216	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0217	<Attribute>
0218	<AttributeName type="TextString" value="Link"/>
0219	<AttributeValue>
0220	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0221	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0222	</AttributeValue>
0223	</Attribute>
0224	</ResponsePayload>
0225	</BatchItem>
0226	<BatchItem>
0227	<Operation type="Enumeration" value="AddAttribute"/>
0228	<UniqueBatchItemID type="ByteString" value="ba865701c7837be2"/>
0229	<ResultStatus type="Enumeration" value="Success"/>
0230	<ResponsePayload>
0231	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0232	<Attribute>
0233	<AttributeName type="TextString" value="Link"/>
0234	<AttributeIndex type="Integer" value="1"/>
0235	<AttributeValue>
0236	<LinkType type="Enumeration" value="CertificateLink"/>
0237	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0238	</AttributeValue>
0239	</Attribute>
0240	</ResponsePayload>

0241	</BatchItem>
0242	</ResponseMessage>
# TIME 4	
0243	<RequestMessage>
0244	<RequestHeader>
0245	<ProtocolVersion>
0246	<ProtocolVersionMajor type="Integer" value="1"/>
0247	<ProtocolVersionMinor type="Integer" value="2"/>
0248	</ProtocolVersion>
0249	<BatchCount type="Integer" value="1"/>
0250	</RequestHeader>
0251	<BatchItem>
0252	<Operation type="Enumeration" value="GetAttributeList"/>
0253	<RequestPayload>
0254	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0255	</RequestPayload>
0256	</BatchItem>
0257	</RequestMessage>
0258	<ResponseMessage>
0259	<ResponseHeader>
0260	<ProtocolVersion>
0261	<ProtocolVersionMajor type="Integer" value="1"/>
0262	<ProtocolVersionMinor type="Integer" value="2"/>
0263	</ProtocolVersion>
0264	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0265	<BatchCount type="Integer" value="1"/>
0266	</ResponseHeader>
0267	<BatchItem>
0268	<Operation type="Enumeration" value="GetAttributeList"/>
0269	<ResultStatus type="Enumeration" value="Success"/>
0270	<ResponsePayload>
0271	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0272	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0273	<AttributeName type="TextString" value="Certificate Length"/>
0274	<AttributeName type="TextString" value="X.509 Certificate
	Identifier"/>
0275	<AttributeName type="TextString" value="X.509 Certificate
	Issuer"/>
0276	<AttributeName type="TextString" value="X.509 Certificate
	Subject"/>
0277	<AttributeName type="TextString" value="Digital Signature
	Algorithm"/>
0278	<AttributeName type="TextString" value="Fresh"/>
0279	<AttributeName type="TextString" value="Certificate Issuer"/>
0280	<AttributeName type="TextString" value="Certificate Type"/>
0281	<AttributeName type="TextString" value="Certificate Subject"/>
0282	<AttributeName type="TextString" value="Certificate
	Identifier"/>
0283	<AttributeName type="TextString" value="State"/>
0284	<AttributeName type="TextString" value="Digest"/>
0285	<AttributeName type="TextString" value="Link"/>
0286	<AttributeName type="TextString" value="Lease Time"/>
0287	<AttributeName type="TextString" value="Initial Date"/>
0288	<AttributeName type="TextString" value="Unique Identifier"/>

0289	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0290	<AttributeName type="TextString" value="Object Type"/>
0291	<AttributeName type="TextString" value="Last Change Date"/>
0292	<AttributeName type="TextString" value="x-ID"/>
0293	</ResponsePayload>
0294	</BatchItem>
0295	</ResponseMessage>
# TIME 5	
0296	<RequestMessage>
0297	<RequestHeader>
0298	<ProtocolVersion>
0299	<ProtocolVersionMajor type="Integer" value="1"/>
0300	<ProtocolVersionMinor type="Integer" value="2"/>
0301	</ProtocolVersion>
0302	<BatchCount type="Integer" value="1"/>
0303	</RequestHeader>
0304	<BatchItem>
0305	<Operation type="Enumeration" value="GetAttributes"/>
0306	<RequestPayload>
0307	<UniqueIdentifier type="TextString"
0308	value="\$UNIQUE_IDENTIFIER_2"/>
0309	<AttributeName type="TextString" value="Certificate
0310	Identifier"/>
0311	<AttributeName type="TextString" value="Certificate Issuer"/>
0312	<AttributeName type="TextString" value="Certificate Subject"/>
0313	<AttributeName type="TextString" value="Certificate Type"/>
0314	<AttributeName type="TextString" value="Digital Signature
0315	Algorithm"/>
0316	<AttributeName type="TextString" value="Cryptographic
0317	Length"/>
0318	</RequestPayload>
0319	</BatchItem>
0320	</RequestMessage>
0321	<ResponseMessage>
0322	<ResponseHeader>
0323	<ProtocolVersion>
0324	<ProtocolVersionMajor type="Integer" value="1"/>
0325	<ProtocolVersionMinor type="Integer" value="2"/>
0326	</ProtocolVersion>
0327	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0328	<BatchCount type="Integer" value="1"/>
0329	</ResponseHeader>
0330	<BatchItem>
0331	<Operation type="Enumeration" value="GetAttributes"/>
0332	<ResultStatus type="Enumeration" value="Success"/>
0333	<ResponsePayload>
0334	<UniqueIdentifier type="TextString"
0335	value="\$UNIQUE_IDENTIFIER_2"/>
0336	<Attribute>
0337	<AttributeName type="TextString" value="Certificate
0338	Identifier"/>
0339	<AttributeValue>
0340	<Issuer type="TextString"
0341	value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0342	<SerialNumber type="TextString" value="01"/>
0343	</AttributeValue>

0337	</Attribute>
0338	<Attribute>
0339	<AttributeName type="TextString" value="Certificate Issuer"/>
0340	<AttributeValue>
0341	<CertificateIssuerDistinguishedName type="TextString" value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0342	</AttributeValue>
0343	</Attribute>
0344	<Attribute>
0345	<AttributeName type="TextString" value="Certificate Subject"/>
0346	<AttributeValue>
0347	<CertificateSubjectDistinguishedName type="TextString" value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0348	</AttributeValue>
0349	</Attribute>
0350	<Attribute>
0351	<AttributeName type="TextString" value="Certificate Type"/>
0352	<AttributeValue type="Enumeration" value="X_509"/>
0353	</Attribute>
0354	<Attribute>
0355	<AttributeName type="TextString" value="Digital Signature Algorithm"/>
0356	<AttributeValue type="Enumeration" value="SHA_1WithRSAEncryption"/>
0357	</Attribute>
0358	<Attribute>
0359	<AttributeName type="TextString" value="Cryptographic Length"/>
0360	<AttributeValue type="Integer" value="2048"/>
0361	</Attribute>
0362	</ResponsePayload>
0363	</BatchItem>
0364	</ResponseMessage>
# TIME 6	
0365	<RequestMessage>
0366	<RequestHeader>
0367	<ProtocolVersion>
0368	<ProtocolVersionMajor type="Integer" value="1"/>
0369	<ProtocolVersionMinor type="Integer" value="2"/>
0370	</ProtocolVersion>
0371	<BatchCount type="Integer" value="1"/>
0372	</RequestHeader>
0373	<BatchItem>
0374	<Operation type="Enumeration" value="Get"/>
0375	<RequestPayload>
0376	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0377	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0378	</RequestPayload>
0379	</BatchItem>
0380	</RequestMessage>
0381	<ResponseMessage>
0382	<ResponseHeader>
0383	<ProtocolVersion>
0384	<ProtocolVersionMajor type="Integer" value="1"/>

0385	<ProtocolVersionMinor type="Integer" value="2"/>
0386	</ProtocolVersion>
0387	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0388	<BatchCount type="Integer" value="1"/>
0389	</ResponseHeader>
0390	<BatchItem>
0391	<Operation type="Enumeration" value="Get"/>
0392	<ResultStatus type="Enumeration" value="Success"/>
0393	<ResponsePayload>
0394	<ObjectType type="Enumeration" value="PrivateKey"/>
0395	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0396	<PrivateKey>
0397	<KeyBlock>
0398	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0399	<KeyValue>
0400	<KeyMaterial type="ByteString"
	value="308204a50201000282010100ab7f161c0042496ccd6c6d4dad9199734353
	57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483
	46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa
	2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650
	89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c
	795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f
	91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281
	5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050
	203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a
	7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f
	a74cde5fdafabdb6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b
	2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0
	e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a
	a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e
	3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78
	965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8
	c3cdc2464744a793713dafb9f1dbc799ff96423fecdd3cba794286bce920f4b5c183f
	99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967
	4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c
	ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064
	b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e
	59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4
	990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766
	b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab
	7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0
	e94adlee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db
	e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa
	e1ebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2
	7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eaeafa922fd75d5b16b1a5
	61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a72
	6a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171
	666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520
	a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a
	1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d34941
	7e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f812
	9c32341a8b44f"/>
0401	</KeyValue>
0402	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0403	<CryptographicLength type="Integer" value="2048"/>
0404	</KeyBlock>

0405	</PrivateKey>
0406	</ResponsePayload>
0407	</BatchItem>
0408	</ResponseMessage>
# TIME 7	
0409	<RequestMessage>
0410	<RequestHeader>
0411	<ProtocolVersion>
0412	<ProtocolVersionMajor type="Integer" value="1"/>
0413	<ProtocolVersionMinor type="Integer" value="2"/>
0414	</ProtocolVersion>
0415	<BatchCount type="Integer" value="1"/>
0416	</RequestHeader>
0417	<BatchItem>
0418	<Operation type="Enumeration" value="Get"/>
0419	<RequestPayload>
0420	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0421	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0422	</RequestPayload>
0423	</BatchItem>
0424	</RequestMessage>
0425	<ResponseMessage>
0426	<ResponseHeader>
0427	<ProtocolVersion>
0428	<ProtocolVersionMajor type="Integer" value="1"/>
0429	<ProtocolVersionMinor type="Integer" value="2"/>
0430	</ProtocolVersion>
0431	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0432	<BatchCount type="Integer" value="1"/>
0433	</ResponseHeader>
0434	<BatchItem>
0435	<Operation type="Enumeration" value="Get"/>
0436	<ResultStatus type="Enumeration" value="Success"/>
0437	<ResponsePayload>
0438	<ObjectType type="Enumeration" value="PublicKey"/>
0439	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0440	<PublicKey>
0441	<KeyBlock>
0442	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0443	<KeyValue>
0444	<KeyMaterial type="ByteString"
	value="3082010a0282010100ab7f161c0042496ccd6c6d4dadb9199734353577760 03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b 8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89 b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981 35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328 abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013 da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612 a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010 001"/>
0445	</KeyValue>
0446	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0447	<CryptographicLength type="Integer" value="2048"/>
0448	</KeyBlock>
0449	</PublicKey>

0450	</ResponsePayload>
0451	</BatchItem>
0452	</ResponseMessage>
0453	# TIME 8
0453	<RequestMessage>
0454	<RequestHeader>
0455	<ProtocolVersion>
0456	<ProtocolVersionMajor type="Integer" value="1"/>
0457	<ProtocolVersionMinor type="Integer" value="2"/>
0458	</ProtocolVersion>
0459	<BatchCount type="Integer" value="1"/>
0460	</RequestHeader>
0461	<BatchItem>
0462	<Operation type="Enumeration" value="Get"/>
0463	<RequestPayload>
0464	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0465	</RequestPayload>
0466	</BatchItem>
0467	</RequestMessage>
0468	<ResponseMessage>
0469	<ResponseHeader>
0470	<ProtocolVersion>
0471	<ProtocolVersionMajor type="Integer" value="1"/>
0472	<ProtocolVersionMinor type="Integer" value="2"/>
0473	</ProtocolVersion>
0474	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0475	<BatchCount type="Integer" value="1"/>
0476	</ResponseHeader>
0477	<BatchItem>
0478	<Operation type="Enumeration" value="Get"/>
0479	<ResultStatus type="Enumeration" value="Success"/>
0480	<ResponsePayload>
0481	<ObjectType type="Enumeration" value="Certificate"/>
0482	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0483	<Certificate>
0484	<CertificateType type="Enumeration" value="X_509"/>
0485	<CertificateValue type="ByteString" value="30820312308201faa003020102020101300d06092a864886f70d010105050 0303b310b3009060355040613025553310d300b060355040a130454455354310e300 c060355040b13054f41534953310d300b060355040313044b4d4950301e170d31303 13130313233353935395a170d3230313130313233353935395a303b310b300906035 5040613025553310d300b060355040a130454455354310e300c060355040b13054f4 1534953310d300b060355040313044b4d495030820122300d06092a864886f70d010 10105000382010f003082010a0282010100ab7f161c0042496ccd6c6d4dad919973 435357776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74 648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc62 67fa2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8 b65089f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295 353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142c b76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1 c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f 6050203010001a321301f301d0603551d0e0416041404e57bd2c431b2e816e180a19 823fac858273f6b300d06092a864886f70d01010505000382010100a876adbc6c8e0 ff017216e195fea76bff61a567c9a13dc50d13fec12a4273c441547cfabcb5d61d99 1e966319df72c0d41ba826a45112ff26089a2344f4d71cf7c921b4bdfaef1600d1ba

0486	aa15336057e014b8b496d4fae9e8a6c1da9aeb6cbc960cbf2fae77f587ec4bb28204
0487	5338845b88dd9aeea53e482a36e734e4f5f03b9d0dfc4cafc6bb34ea9053e52bd609
0488	ee01e86d9b09fb51120c19834a997b09ce08d79e81311762f974bb1c8c09186c4d78
0489	933e0db38e905084877e147c78af52fae07192ff166d19fa94a11cc11b27ed050f7a
	27fae13b205a574c4ee00aa8bd65d0d7057c985c839ef336a441ed53a53c6b6b696f
	1bdeb5f7ea811ebb25a7f86"/>
	</Certificate>
	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>
0490	# TIME 9
0491	<RequestMessage>
0492	<RequestHeader>
0493	<ProtocolVersion>
0494	<ProtocolVersionMajor type="Integer" value="1"/>
0495	<ProtocolVersionMinor type="Integer" value="2"/>
0496	</ProtocolVersion>
0497	<BatchCount type="Integer" value="1"/>
0498	</RequestHeader>
0499	<BatchItem>
0500	<Operation type="Enumeration" value="Destroy"/>
0501	<RequestPayload>
0502	<UniqueIdentifier type="TextString"
0503	value="\$UNIQUE_IDENTIFIER_1"/>
0504	</RequestPayload>
0505	</BatchItem>
0506	</RequestMessage>
0507	<ResponseMessage>
0508	<ResponseHeader>
0509	<ProtocolVersion>
0510	<ProtocolVersionMajor type="Integer" value="1"/>
0511	<ProtocolVersionMinor type="Integer" value="2"/>
0512	</ProtocolVersion>
0513	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0514	<BatchCount type="Integer" value="1"/>
0515	</ResponseHeader>
0516	<BatchItem>
0517	<Operation type="Enumeration" value="Destroy"/>
0518	<ResultStatus type="Enumeration" value="Success"/>
0519	<ResponsePayload>
0520	<UniqueIdentifier type="TextString"
0521	value="\$UNIQUE_IDENTIFIER_1"/>
0522	</ResponsePayload>
0523	</BatchItem>
0524	</ResponseMessage>
0525	# TIME 10
0526	<RequestMessage>
0527	<RequestHeader>
0528	<ProtocolVersion>
0529	<ProtocolVersionMajor type="Integer" value="1"/>
0530	<ProtocolVersionMinor type="Integer" value="2"/>
0531	</ProtocolVersion>
	<BatchCount type="Integer" value="1"/>
	</RequestHeader>
	<BatchItem>
	<Operation type="Enumeration" value="Destroy"/>

0532	<RequestPayload>
0533	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0534	</RequestPayload>
0535	</BatchItem>
0536	</RequestMessage>
0537	<ResponseMessage>
0538	<ResponseHeader>
0539	<ProtocolVersion>
0540	<ProtocolVersionMajor type="Integer" value="1"/>
0541	<ProtocolVersionMinor type="Integer" value="2"/>
0542	</ProtocolVersion>
0543	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0544	<BatchCount type="Integer" value="1"/>
0545	</ResponseHeader>
0546	<BatchItem>
0547	<Operation type="Enumeration" value="Destroy"/>
0548	<ResultStatus type="Enumeration" value="Success"/>
0549	<ResponsePayload>
0550	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0551	</ResponsePayload>
0552	</BatchItem>
0553	</ResponseMessage>
	# TIME 11
0554	<RequestMessage>
0555	<RequestHeader>
0556	<ProtocolVersion>
0557	<ProtocolVersionMajor type="Integer" value="1"/>
0558	<ProtocolVersionMinor type="Integer" value="2"/>
0559	</ProtocolVersion>
0560	<BatchCount type="Integer" value="1"/>
0561	</RequestHeader>
0562	<BatchItem>
0563	<Operation type="Enumeration" value="Destroy"/>
0564	<RequestPayload>
0565	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0566	</RequestPayload>
0567	</BatchItem>
0568	</RequestMessage>
0569	<ResponseMessage>
0570	<ResponseHeader>
0571	<ProtocolVersion>
0572	<ProtocolVersionMajor type="Integer" value="1"/>
0573	<ProtocolVersionMinor type="Integer" value="2"/>
0574	</ProtocolVersion>
0575	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0576	<BatchCount type="Integer" value="1"/>
0577	</ResponseHeader>
0578	<BatchItem>
0579	<Operation type="Enumeration" value="Destroy"/>
0580	<ResultStatus type="Enumeration" value="Success"/>
0581	<ResponsePayload>
0582	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>

0583	<code></ResponsePayload></code>
0584	<code></BatchItem></code>
0585	<code></ResponseMessage></code>

936

937 2.3.26 TC-133-12 - Create, Re-key Key Pair

938 Create a public/private key pair on the server and retrieve the keys in PKCS_1 format. Re-key the
939 key pair and retrieve the new public/private key pair in transparent format. To verify that the
940 links are set correctly, the Link attributes are retrieved. Finally, all the keys are destroyed.

941 Note: a server is not required to support conversion between key formats so returning keys in
942 Transparent form when registered in PKCS_1 may not be supported.

	<code># TIME 0</code>
0001	<code><RequestMessage></code>
0002	<code><RequestHeader></code>
0003	<code><ProtocolVersion></code>
0004	<code><ProtocolVersionMajor type="Integer" value="1"/></code>
0005	<code><ProtocolVersionMinor type="Integer" value="2"/></code>
0006	<code></ProtocolVersion></code>
0007	<code><BatchCount type="Integer" value="1"/></code>
0008	<code></RequestHeader></code>
0009	<code><BatchItem></code>
0010	<code><Operation type="Enumeration" value="CreateKeyPair"/></code>
0011	<code><RequestPayload></code>
0012	<code><CommonTemplateAttribute></code>
0013	<code><Attribute></code>
0014	<code><AttributeName type="TextString" value="Cryptographic</code>
	<code>Algorithm"/></code>
0015	<code><AttributeValue type="Enumeration" value="RSA"/></code>
0016	<code></Attribute></code>
0017	<code><Attribute></code>
0018	<code><AttributeName type="TextString" value="Cryptographic</code>
	<code>Length"/></code>
0019	<code><AttributeValue type="Integer" value="2048"/></code>
0020	<code></Attribute></code>
0021	<code></CommonTemplateAttribute></code>
0022	<code><PrivateKeyTemplateAttribute></code>
0023	<code><Attribute></code>
0024	<code><AttributeName type="TextString" value="Name"/></code>
0025	<code><AttributeValue></code>
0026	<code><NameValue type="TextString" value="TC-133-12-</code>
	<code>privateKey1"/></code>
0027	<code><NameType type="Enumeration"</code>
	<code>value="UninterpretedTextString"/></code>
0028	<code></AttributeValue></code>
0029	<code></Attribute></code>
0030	<code><Attribute></code>
0031	<code><AttributeName type="TextString" value="Cryptographic</code>
	<code>Usage Mask"/></code>
0032	<code><AttributeValue type="Integer" value="Sign"/></code>
0033	<code></Attribute></code>
0034	<code></PrivateKeyTemplateAttribute></code>
0035	<code><PublicKeyTemplateAttribute></code>

0036	<Attribute>
0037	<AttributeName type="TextString" value="Name"/>
0038	<AttributeValue>
0039	<NameValue type="TextString" value="TC-133-12- publicKey1"/>
0040	<NameType type="Enumeration" value="UninterpretedTextString"/>
0041	</AttributeValue>
0042	</Attribute>
0043	<Attribute>
0044	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0045	<AttributeValue type="Integer" value="Verify"/>
0046	</Attribute>
0047	</PublicKeyTemplateAttribute>
0048	</RequestPayload>
0049	</BatchItem>
0050	</RequestMessage>
0051	<ResponseMessage>
0052	<ResponseHeader>
0053	<ProtocolVersion>
0054	<ProtocolVersionMajor type="Integer" value="1"/>
0055	<ProtocolVersionMinor type="Integer" value="2"/>
0056	</ProtocolVersion>
0057	<TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/>
0058	<BatchCount type="Integer" value="1"/>
0059	</ResponseHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="CreateKeyPair"/>
0062	<ResultStatus type="Enumeration" value="Success"/>
0063	<ResponsePayload>
0064	<PrivateKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0065	<PublicKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
	# TIME 1
0069	<RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="2"/>
0074	</ProtocolVersion>
0075	<BatchCount type="Integer" value="1"/>
0076	</RequestHeader>
0077	<BatchItem>
0078	<Operation type="Enumeration" value="Get"/>
0079	<RequestPayload>
0080	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0081	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0082	</RequestPayload>
0083	</BatchItem>
0084	</RequestMessage>

```
0085 <ResponseMessage>
0086   <ResponseHeader>
0087     <ProtocolVersion>
0088       <ProtocolVersionMajor type="Integer" value="1"/>
0089       <ProtocolVersionMinor type="Integer" value="2"/>
0090     </ProtocolVersion>
0091     <TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/>
0092     <BatchCount type="Integer" value="1"/>
0093   </ResponseHeader>
0094   <BatchItem>
0095     <Operation type="Enumeration" value="Get"/>
0096     <ResultStatus type="Enumeration" value="Success"/>
0097     <ResponsePayload>
0098       <ObjectType type="Enumeration" value="PrivateKey"/>
0099       <UniqueIdentifier type="TextString"
0100         value="$UNIQUE_IDENTIFIER_0"/>
0101       <PrivateKey>
0102         <KeyBlock>
0103           <KeyFormatType type="Enumeration" value="PKCS_1"/>
0104           <KeyValue>
0105             <KeyMaterial type="ByteString"
0106               value="308204a30201000282010100b0612bccafdd11d41819a274526d68dbf3c3f
0107 25667c402a0e0e8e4cce007ea6b6ea53699e8bd7ccab7d5ae66c00b28fd678b81ba1
0108 d4e841c3a36caf13f852004633f80d840be7aad9bcdeabde11514b6ab3bce602e113
0109 05cf5e9c34abee32c3c468b9b146502738c0ae82e63ab8bd1fc4db0c6a09eb0c9f6e
0110 01b9cc8d22317aedab328209a1dc5d2ce8529d81521c41730c1c8c76249d233e8909
0111 6ca44dfefb469e3532bb90d6691c6932d0c63dbb7647c6e64337b719a1f100b1366cf
0112 f3bbb213b17c716beb2c9ad88b3b76abacc378c4898636480fff1108e1fa1e7573c0
0113 96606e21b18a05245ebd976701bb676dc2962a328d39385ef7571bc48ae134b37410
0114 2030100010282010037b71a3cd838bf0efe65ea9950085b9d4f4d5059d70165cb280
0115 0a975c636f9e7e1d5b27fbfb34b9e459fec2d6cf0998c228f40f567988bc6d6e4c40
0116 a9d04126f1062d8f276d134b36e8a0762df9ce72424c70993fc3955cba7aaa61553d
0117 b32f7ff58ce2e0d124f29a7b05c2703e370fb80171d47539988d2c14c37a4802cb1a
0118 7f5685bcc78865480ca4e5d367cafca8b533e610620f94f54a082effc4c4e50998410
0119 dd32fa7dedae895200b56437fe177f47d1b373b5e8e0c62f64b3a19e5918be83e90a
0120 1bbe195a4b516f3ceae6db35b0e4427858631dcbce6b1e49cf12345297df41e54d2c
0121 bc2834c34e37bb92888e4659d232a4f3d22edeb9bffa43b7881c7902818100eab3861
0122 80dec393c70c8b00c5fae6a10e6b620ae82e5096ce11bf4c539a015165a7481227e9
0123 1492748159d85317d1e81b780cca1cf19630a10987b940663a2496a4ead2ed4bfb70
0124 17dc813e7a49017aa278b8ac1381ef27fde54ed4alee1e74812dcae514cb9d48590
0125 eb3972b26ba2f21de0aab64cfc1dbcba32561f5f31d6f02818100c062be5756e93eb
0126 e005be752a5b7be2d35b342e483ff266cc9f595edbcffff603c8e03dcd9350a19fab
0127 f434077f9543088132f0e843c2da6fe4f1cedee49a5eb9a8aea1219a41c1db392521
0128 96137a041def9edcfff43aa9280d90be137dbf48777e6055695f58fcc9cd6b07924fd
0129 ab47a5553f5ad7b82d52553f6ec3f647ffe4f0281804221676d2baf1dc97bf5f034e
0130 c58d6a6007bdce58f183df9a1cc20c1d9a4d38c42dc84ee553f569f6cde3a4e274d9
0131 be4ecf1abb70405a1345accbc354f3f8fa0a4059b2290eb9c031d8fdc9bee70735a8
0132 c5df330d241560ed574948fc7f7db1521cb70b43791cfb56cf28983d4b2cacf30f9c
0133 183dd99f4839bf3523b31f3d89d0281806cbe63c0928bbcbf410cb1b071a36e87bf77
0134 6e034b2b7a24c93cb913794414f64625613b0ddc5b134061bde33ae9cec0d929ce55
0135 85b3e78bf8fb7c02e6d268bf6a4a028b69a6fbcc4bd1fd3f02c9778aa43131a6d152
0136 ba339d491201f7c5086f1a429679dec1b2ca814c88ebb11101a3b9bc79d72b601b9e
0137 12398cae8fa31aed90281810099777cd45f0d1a862888eb2cf7ac14d22d75b88e99a
0138 df66f15cccbd29979bf5eaa90bb8c29b29a8be1257425a9a2db2f493df4a740c7fbc
0139 138e4b4d80f24e7ca11d63528d900ba2dd5c44da59e2d601544ec92681161f17b86c
0140 838694a49a978f76ff05287bfce0704c6f3f9fa87551d0cfla970b2cb130b5320783
0141 a36ea8613"/>
0142           </KeyMaterial>
0143         </KeyValue>
0144       </KeyBlock>
0145     </PrivateKey>
0146   </BatchItem>
0147 </ResponsePayload>
0148 </BatchItem>
0149 </ResponseMessage>
```

0105	</KeyValue>
0106	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0107	<CryptographicLength type="Integer" value="2048"/>
0108	</KeyBlock>
0109	</PrivateKey>
0110	</ResponsePayload>
0111	</BatchItem>
0112	</ResponseMessage>
# TIME 2	
0113	<RequestMessage>
0114	<RequestHeader>
0115	<ProtocolVersion>
0116	<ProtocolVersionMajor type="Integer" value="1"/>
0117	<ProtocolVersionMinor type="Integer" value="2"/>
0118	</ProtocolVersion>
0119	<BatchCount type="Integer" value="1"/>
0120	</RequestHeader>
0121	<BatchItem>
0122	<Operation type="Enumeration" value="Get"/>
0123	<RequestPayload>
0124	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0125	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0126	</RequestPayload>
0127	</BatchItem>
0128	</RequestMessage>
0129	<ResponseMessage>
0130	<ResponseHeader>
0131	<ProtocolVersion>
0132	<ProtocolVersionMajor type="Integer" value="1"/>
0133	<ProtocolVersionMinor type="Integer" value="2"/>
0134	</ProtocolVersion>
0135	<TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/>
0136	<BatchCount type="Integer" value="1"/>
0137	</ResponseHeader>
0138	<BatchItem>
0139	<Operation type="Enumeration" value="Get"/>
0140	<ResultStatus type="Enumeration" value="Success"/>
0141	<ResponsePayload>
0142	<ObjectType type="Enumeration" value="PublicKey"/>
0143	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0144	<PublicKey>
0145	<KeyBlock>
0146	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0147	<KeyValue>
0148	<KeyMaterial type="ByteString" value="3082010a0282010100b0612bccafdd11d41819a274526d68dbf3c3f25667c 402a0e0e8e4cce007ea6b6ea53699e8bd7ccab7d5ae66c00b28fd678b81ba1d4e841 c3a36caf13f852004633f80d840be7aad9bcbdeabdel1514b6ab3bce602e11305cf5e 9c34ebee32c3c468b9b146502738c0ae82e63ab8bd1fc4db0c6a09eb0c9f6e01b9cc 8d22317aedab328209a1dc5d2ce8529d81521c41730c1c8c76249d233e89096ca44d feb469e3532bb90d6691c6932d0c63dbb7647c6e64337b719a1f100b1366cff3bbb2 13b17c716beb2c9ad88b3b76abacc378c4898636480fff1108e1fa1e7573c096606e 21b18a05245ebd976701bb676dc2962a328d39385ef7571bc48ae134b37410203010 001"/>
0149	</KeyValue>

0150	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0151	<CryptographicLength type="Integer" value="2048"/>
0152	</KeyBlock>
0153	</PublicKey>
0154	</ResponsePayload>
0155	</BatchItem>
0156	</ResponseMessage>
# TIME 3	
0157	<RequestMessage>
0158	<RequestHeader>
0159	<ProtocolVersion>
0160	<ProtocolVersionMajor type="Integer" value="1"/>
0161	<ProtocolVersionMinor type="Integer" value="2"/>
0162	</ProtocolVersion>
0163	<BatchCount type="Integer" value="1"/>
0164	</RequestHeader>
0165	<BatchItem>
0166	<Operation type="Enumeration" value="ReKeyKeyPair"/>
0167	<RequestPayload>
0168	<PrivateKeyUniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0169	</RequestPayload>
0170	</BatchItem>
0171	</RequestMessage>
0172	<ResponseMessage>
0173	<ResponseHeader>
0174	<ProtocolVersion>
0175	<ProtocolVersionMajor type="Integer" value="1"/>
0176	<ProtocolVersionMinor type="Integer" value="2"/>
0177	</ProtocolVersion>
0178	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0179	<BatchCount type="Integer" value="1"/>
0180	</ResponseHeader>
0181	<BatchItem>
0182	<Operation type="Enumeration" value="ReKeyKeyPair"/>
0183	<ResultStatus type="Enumeration" value="Success"/>
0184	<ResponsePayload>
0185	<PrivateKeyUniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0186	<PublicKeyUniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0187	</ResponsePayload>
0188	</BatchItem>
0189	</ResponseMessage>
# TIME 4	
0190	<RequestMessage>
0191	<RequestHeader>
0192	<ProtocolVersion>
0193	<ProtocolVersionMajor type="Integer" value="1"/>
0194	<ProtocolVersionMinor type="Integer" value="2"/>
0195	</ProtocolVersion>
0196	<BatchOrderOption type="Boolean" value="true"/>
0197	<BatchCount type="Integer" value="2"/>
0198	</RequestHeader>
0199	<BatchItem>
0200	<Operation type="Enumeration" value="Locate"/>

0201	<UniqueBatchItemID type="ByteString" value="f409f9adc43f836f"/>
0202	<RequestPayload>
0203	<MaximumItems type="Integer" value="1"/>
0204	<Attribute>
0205	<AttributeName type="TextString" value="Name"/>
0206	<AttributeValue>
0207	<NameValue type="TextString" value="TC-133-12-privateKey1"/>
0208	<NameType type="Enumeration" value="UninterpretedTextString"/>
0209	</AttributeValue>
0210	</Attribute>
0211	<Attribute>
0212	<AttributeName type="TextString" value="Object Type"/>
0213	<AttributeValue type="Enumeration" value="PrivateKey"/>
0214	</Attribute>
0215	</RequestPayload>
0216	</BatchItem>
0217	<BatchItem>
0218	<Operation type="Enumeration" value="Get"/>
0219	<UniqueBatchItemID type="ByteString" value="396c4d8b5bde0667"/>
0220	<RequestPayload>
0221	<KeyFormatType type="Enumeration" value="TransparentRSAPrivateKey"/>
0222	</RequestPayload>
0223	</BatchItem>
0224	</RequestMessage>
0225	<ResponseMessage>
0226	<ResponseHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="2"/>
0230	</ProtocolVersion>
0231	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0232	<BatchCount type="Integer" value="2"/>
0233	</ResponseHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="Locate"/>
0236	<UniqueBatchItemID type="ByteString" value="f409f9adc43f836f"/>
0237	<ResultStatus type="Enumeration" value="Success"/>
0238	<ResponsePayload>
0239	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0240	</ResponsePayload>
0241	</BatchItem>
0242	<BatchItem>
0243	<Operation type="Enumeration" value="Get"/>
0244	<UniqueBatchItemID type="ByteString" value="396c4d8b5bde0667"/>
0245	<ResultStatus type="Enumeration" value="Success"/>
0246	<ResponsePayload>
0247	<ObjectType type="Enumeration" value="PrivateKey"/>
0248	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0249	<PrivateKey>
0250	<KeyBlock>
0251	<KeyFormatType type="Enumeration" value="TransparentRSAPrivateKey"/>

0252	<KeyValue>
0253	<KeyMaterial>
0254	<Modulus type="BigInteger" value="0000000000000000eab4492bbb2364359408c57b8af47003572c81aaed719 ed92d9b13c741cc196b717d1c98f0c250580e37ac3ade11a7cd1aaede3a0424b53d3 3200510ce7eef71ded7e96e585d1d7ba3767a8dbfad4d2701b5831a34552a827fc2c d398e659fd5063e1dfd28a994b0e6a7449bbad8dcf40e22943b841aa9e58519fa357 5b4409abfeb57f5723b45f7ce4e5277a2d0acccbcd49608d6ff8a7c933d4d70a9e8c 8df24829b58404a5af1b0d4c8668c35e3549e28204f2249bfc13b20c05ab0252c975 e53f604f68c6e498c7b14adb72debac91221a8eb1ad581080144eb8900b4bf9d9792 be37ec6191ad183e2b60b80174eecb66ca08c3ac07f51ba1c056130ec69"/>
0255	<PrivateExponent type="BigInteger" value="42e22587e4c86d2227916855907f9ffc13b7872c228622725960bbfe286df 5407d12de376744b8889f64961c20747f911f6d7dbea2b7a33e51776a7a239e60b5d e7f40f2451423f6bbda638a497925675c41519f0212d30e65422a21a0c6ad0993c1d 7e1f0d8829af6dfebd94521cfb56ce1c5c4401d2915531cd804ac0a35ee57d2a43ff d7671aeaad0ab090f17f8419073445ac6fb218bd3c7c5beb9f3e7bf41e4e5f9632d8 492eb0cb2ada41083e040535ae409ad866d1998a0335f253cda2d21a95b2feebacee 64b969aaccab322fa0ecbc75c3f0c15c267dbf431abedecae191b72000b612e41e65 eb93c9f08eef67740b84ba32d9c5697ed91e1c8ccd1"/>
0256	<PublicExponent type="BigInteger" value="0000000000010001"/>
0257	<P type="BigInteger" value="0000000000000000f88c737435b8b3f5bdb2b2eb73dd5a665e2ee56c64e05 5169038f754ed3021d3e72ae82234dacd4a5fa12edeb4874b70c5915bba4571bef55 964389d8a4b8a79b628771bb4d634fbd18a27ab5fb6973309c4af9e27d269b1c4054 b62012d1c52847e3679f71f91cf7ff6b646c9edaafe5b46845fc1190fa0ef80b8a45 de63973"/>
0258	<Q type="BigInteger" value="0000000000000000f1bd952150d189707c316486f205429680230505581b4 0ed503901bef82cec4e2a0a564c58365e8c82b7d34a0305d407194b1d15c273015d1 212969906267322827303b276d0c7585a21ee6758a74e95bfec5b544686325754e5 d2602f0d5734c58f870aa2ca00e08122e940e4d6d0e11611d47966482df8845b8ff8 8d1fbb3"/>
0259	<PrimeExponentP type="BigInteger" value="0000000000000000e9717156eac62a305b15a63ac33e5a13dfce0829c0ad7 afd904410f9b1350df0ab247f96f131b8b36c1245a562c5d833793cc77cb290dd1c2 ff393c1540d1368b1905c1ea7c0b14efb45d9707a9b5273db6ee2cb96f767d2511be feb82d34dd0ab24a821f1dbb2e5c3788347058db696e43fdd40da6aa16534celf9e3 19b74c5"/>
0260	<PrimeExponentQ type="BigInteger" value="0000000000000000eb6294819a364dc3afca507e6dcedd65ba635f1233166 6842d6734e204b989671adc71e768c5980eed819d4525e858ea88a07133ace15ae48 b227a6d8a658a1a823707d49088fe72736132c882b4767aae2518e64633f6c69490b 776b9ca53ad2f1c3add4976a66ac34521019d639adae5e5502352b7900fa49b6f65b 28df4ad"/>
0261	<CRTCoefficient type="BigInteger" value="0000000000000000cc75a52cab58eb65878acf7c19070c0a495d5376f40b8 6531b98b1e3b44e28d39db55898db8aa317ce214814efdd00c1d234d4c27168710a1 a68cfdae310f1a56e17e1a51f43d069137beeb7a6aeef4da2b3dfde54d222e24c772 09dc5c8c831b8f09f816d3ee628e76e93bae2594229a59b36ealf507be2db99ae358 896956e"/>
0262	</KeyMaterial>
0263	</KeyValue>
0264	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0265	<CryptographicLength type="Integer" value="2048"/>
0266	</KeyBlock>

0267	</PrivateKey>
0268	</ResponsePayload>
0269	</BatchItem>
0270	</ResponseMessage>
# TIME 5	
0271	<RequestMessage>
0272	<RequestHeader>
0273	<ProtocolVersion>
0274	<ProtocolVersionMajor type="Integer" value="1"/>
0275	<ProtocolVersionMinor type="Integer" value="2"/>
0276	</ProtocolVersion>
0277	<BatchOrderOption type="Boolean" value="true"/>
0278	<BatchCount type="Integer" value="2"/>
0279	</RequestHeader>
0280	<BatchItem>
0281	<Operation type="Enumeration" value="Locate"/>
0282	<UniqueBatchItemID type="ByteString" value="5df01d7748d64a16"/>
0283	<RequestPayload>
0284	<MaximumItems type="Integer" value="1"/>
0285	<Attribute>
0286	<AttributeName type="TextString" value="Name"/>
0287	<AttributeValue>
0288	<NameValue type="TextString" value="TC-133-12- publicKey1"/>
0289	<NameType type="Enumeration" value="UninterpretedTextString"/>
0290	</AttributeValue>
0291	</Attribute>
0292	<Attribute>
0293	<AttributeName type="TextString" value="Object Type"/>
0294	<AttributeValue type="Enumeration" value="PublicKey"/>
0295	</Attribute>
0296	</RequestPayload>
0297	</BatchItem>
0298	<BatchItem>
0299	<Operation type="Enumeration" value="Get"/>
0300	<UniqueBatchItemID type="ByteString" value="7c7f588280a61c24"/>
0301	<RequestPayload>
0302	<KeyFormatType type="Enumeration" value="TransparentRSAPublicKey"/>
0303	</RequestPayload>
0304	</BatchItem>
0305	</RequestMessage>
0306	<ResponseMessage>
0307	<ResponseHeader>
0308	<ProtocolVersion>
0309	<ProtocolVersionMajor type="Integer" value="1"/>
0310	<ProtocolVersionMinor type="Integer" value="2"/>
0311	</ProtocolVersion>
0312	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0313	<BatchCount type="Integer" value="2"/>
0314	</ResponseHeader>
0315	<BatchItem>
0316	<Operation type="Enumeration" value="Locate"/>
0317	<UniqueBatchItemID type="ByteString" value="5df01d7748d64a16"/>
0318	<ResultStatus type="Enumeration" value="Success"/>
0319	<ResponsePayload>

0320	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0321	</ResponsePayload>
0322	</BatchItem>
0323	<BatchItem>
0324	<Operation type="Enumeration" value="Get"/>
0325	<UniqueBatchItemID type="ByteString" value="7c7f588280a61c24"/>
0326	<ResultStatus type="Enumeration" value="Success"/>
0327	<ResponsePayload>
0328	<ObjectType type="Enumeration" value="PublicKey"/>
0329	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0330	<PublicKey>
0331	<KeyBlock>
0332	<KeyFormatType type="Enumeration"
	value="TransparentRSAPublicKey"/>
0333	<KeyValue>
0334	<KeyMaterial>
0335	<Modulus type="BigInteger"
	value="0000000000000000eab4492bbb2364359408c57b8af47003572c81aaed719 ed92d9b13c741cc196b717d1c98f0c250580e37ac3ade11a7cd1aaede3a0424b53d3 3200510ce7eef71ded7e96e585d1d7ba3767a8dbfad4d2701b5831a34552a827fc2c d398e659fd5063e1dfd28a994b0e6a7449bbad8dcf40e22943b841aa9e58519fa357 5b4409abfeb57f5723b45f7ce4e5277a2d0accbcbcd49608d6ff8a7c933d4d70a9e8c 8df24829b58404a5af1b0d4c8668c35e3549e28204f2249bfc13b20c05ab0252c975 e53f604f68c6e498c7b14adb72debac91221a8eb1ad581080144eb8900b4bfb9d9792 be37ec6191ad183e2b60b80174eeeb66ca08c3ac07f51ba1c056130ec69"/>
0336	<PublicExponent type="BigInteger"
	value="0000000000010001"/>
0337	</KeyMaterial>
0338	</KeyValue>
0339	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0340	<CryptographicLength type="Integer" value="2048"/>
0341	</KeyBlock>
0342	</PublicKey>
0343	</ResponsePayload>
0344	</BatchItem>
0345	</ResponseMessage>
	# TIME 6
0346	<RequestMessage>
0347	<RequestHeader>
0348	<ProtocolVersion>
0349	<ProtocolVersionMajor type="Integer" value="1"/>
0350	<ProtocolVersionMinor type="Integer" value="2"/>
0351	</ProtocolVersion>
0352	<BatchCount type="Integer" value="1"/>
0353	</RequestHeader>
0354	<BatchItem>
0355	<Operation type="Enumeration" value="GetAttributes"/>
0356	<RequestPayload>
0357	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0358	<AttributeName type="TextString" value="Link"/>
0359	</RequestPayload>
0360	</BatchItem>
0361	</RequestMessage>
0362	<ResponseMessage>

0363	<ResponseHeader>
0364	<ProtocolVersion>
0365	<ProtocolVersionMajor type="Integer" value="1"/>
0366	<ProtocolVersionMinor type="Integer" value="2"/>
0367	</ProtocolVersion>
0368	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0369	<BatchCount type="Integer" value="1"/>
0370	</ResponseHeader>
0371	<BatchItem>
0372	<Operation type="Enumeration" value="GetAttributes"/>
0373	<ResultStatus type="Enumeration" value="Success"/>
0374	<ResponsePayload>
0375	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0376	<Attribute>
0377	<AttributeName type="TextString" value="Link"/>
0378	<AttributeValue>
0379	<LinkType type="Enumeration" value="PublicKeyLink"/>
0380	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0381	</AttributeValue>
0382	</Attribute>
0383	<Attribute>
0384	<AttributeName type="TextString" value="Link"/>
0385	<AttributeIndex type="Integer" value="1"/>
0386	<AttributeValue>
0387	<LinkType type="Enumeration" value="ReplacedObjectLink"/>
0388	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0389	</AttributeValue>
0390	</Attribute>
0391	</ResponsePayload>
0392	</BatchItem>
0393	</ResponseMessage>
# TIME 7	
0394	<RequestMessage>
0395	<RequestHeader>
0396	<ProtocolVersion>
0397	<ProtocolVersionMajor type="Integer" value="1"/>
0398	<ProtocolVersionMinor type="Integer" value="2"/>
0399	</ProtocolVersion>
0400	<BatchCount type="Integer" value="1"/>
0401	</RequestHeader>
0402	<BatchItem>
0403	<Operation type="Enumeration" value="GetAttributes"/>
0404	<RequestPayload>
0405	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0406	<AttributeName type="TextString" value="Link"/>
0407	</RequestPayload>
0408	</BatchItem>
0409	</RequestMessage>
0410	<ResponseMessage>
0411	<ResponseHeader>
0412	<ProtocolVersion>
0413	<ProtocolVersionMajor type="Integer" value="1"/>
0414	<ProtocolVersionMinor type="Integer" value="2"/>

0415	</ProtocolVersion>
0416	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0417	<BatchCount type="Integer" value="1"/>
0418	</ResponseHeader>
0419	<BatchItem>
0420	<Operation type="Enumeration" value="GetAttributes"/>
0421	<ResultStatus type="Enumeration" value="Success"/>
0422	<ResponsePayload>
0423	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0424	<Attribute>
0425	<AttributeName type="TextString" value="Link"/>
0426	<AttributeValue>
0427	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0428	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0429	</AttributeValue>
0430	</Attribute>
0431	<Attribute>
0432	<AttributeName type="TextString" value="Link"/>
0433	<AttributeIndex type="Integer" value="1"/>
0434	<AttributeValue>
0435	<LinkType type="Enumeration" value="ReplacedObjectLink"/>
0436	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0437	</AttributeValue>
0438	</Attribute>
0439	</ResponsePayload>
0440	</BatchItem>
0441	</ResponseMessage>
	# TIME 8
0442	<RequestMessage>
0443	<RequestHeader>
0444	<ProtocolVersion>
0445	<ProtocolVersionMajor type="Integer" value="1"/>
0446	<ProtocolVersionMinor type="Integer" value="2"/>
0447	</ProtocolVersion>
0448	<BatchCount type="Integer" value="1"/>
0449	</RequestHeader>
0450	<BatchItem>
0451	<Operation type="Enumeration" value="GetAttributes"/>
0452	<RequestPayload>
0453	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0454	<AttributeName type="TextString" value="Link"/>
0455	</RequestPayload>
0456	</BatchItem>
0457	</RequestMessage>
0458	<ResponseMessage>
0459	<ResponseHeader>
0460	<ProtocolVersion>
0461	<ProtocolVersionMajor type="Integer" value="1"/>
0462	<ProtocolVersionMinor type="Integer" value="2"/>
0463	</ProtocolVersion>
0464	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0465	<BatchCount type="Integer" value="1"/>
0466	</ResponseHeader>

0467	<BatchItem>
0468	<Operation type="Enumeration" value="GetAttributes"/>
0469	<ResultStatus type="Enumeration" value="Success"/>
0470	<ResponsePayload>
0471	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0472	<Attribute>
0473	<AttributeName type="TextString" value="Link"/>
0474	<AttributeValue>
0475	<LinkType type="Enumeration" value="PublicKeyLink"/>
0476	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0477	</AttributeValue>
0478	</Attribute>
0479	<Attribute>
0480	<AttributeName type="TextString" value="Link"/>
0481	<AttributeIndex type="Integer" value="1"/>
0482	<AttributeValue>
0483	<LinkType type="Enumeration"
	value="ReplacementObjectLink"/>
0484	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0485	</AttributeValue>
0486	</Attribute>
0487	</ResponsePayload>
0488	</BatchItem>
0489	</ResponseMessage>
# TIME 9	
0490	<RequestMessage>
0491	<RequestHeader>
0492	<ProtocolVersion>
0493	<ProtocolVersionMajor type="Integer" value="1"/>
0494	<ProtocolVersionMinor type="Integer" value="2"/>
0495	</ProtocolVersion>
0496	<BatchCount type="Integer" value="1"/>
0497	</RequestHeader>
0498	<BatchItem>
0499	<Operation type="Enumeration" value="GetAttributes"/>
0500	<RequestPayload>
0501	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0502	<AttributeName type="TextString" value="Link"/>
0503	</RequestPayload>
0504	</BatchItem>
0505	</RequestMessage>
0506	<ResponseMessage>
0507	<ResponseHeader>
0508	<ProtocolVersion>
0509	<ProtocolVersionMajor type="Integer" value="1"/>
0510	<ProtocolVersionMinor type="Integer" value="2"/>
0511	</ProtocolVersion>
0512	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0513	<BatchCount type="Integer" value="1"/>
0514	</ResponseHeader>
0515	<BatchItem>
0516	<Operation type="Enumeration" value="GetAttributes"/>
0517	<ResultStatus type="Enumeration" value="Success"/>

0518	<ResponsePayload>
0519	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0520	<Attribute>
0521	<AttributeName type="TextString" value="Link"/>
0522	<AttributeValue>
0523	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0524	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0525	</AttributeValue>
0526	</Attribute>
0527	<Attribute>
0528	<AttributeName type="TextString" value="Link"/>
0529	<AttributeIndex type="Integer" value="1"/>
0530	<AttributeValue>
0531	<LinkType type="Enumeration"
	value="ReplacementObjectLink"/>
0532	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0533	</AttributeValue>
0534	</Attribute>
0535	</ResponsePayload>
0536	</BatchItem>
0537	</ResponseMessage>
# TIME 10	
0538	<RequestMessage>
0539	<RequestHeader>
0540	<ProtocolVersion>
0541	<ProtocolVersionMajor type="Integer" value="1"/>
0542	<ProtocolVersionMinor type="Integer" value="2"/>
0543	</ProtocolVersion>
0544	<BatchCount type="Integer" value="1"/>
0545	</RequestHeader>
0546	<BatchItem>
0547	<Operation type="Enumeration" value="Destroy"/>
0548	<RequestPayload>
0549	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0550	</RequestPayload>
0551	</BatchItem>
0552	</RequestMessage>
0553	<ResponseMessage>
0554	<ResponseHeader>
0555	<ProtocolVersion>
0556	<ProtocolVersionMajor type="Integer" value="1"/>
0557	<ProtocolVersionMinor type="Integer" value="2"/>
0558	</ProtocolVersion>
0559	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0560	<BatchCount type="Integer" value="1"/>
0561	</ResponseHeader>
0562	<BatchItem>
0563	<Operation type="Enumeration" value="Destroy"/>
0564	<ResultStatus type="Enumeration" value="Success"/>
0565	<ResponsePayload>
0566	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0567	</ResponsePayload>

0568	</BatchItem>
0569	</ResponseMessage>
# TIME 11	
0570	<RequestMessage>
0571	<RequestHeader>
0572	<ProtocolVersion>
0573	<ProtocolVersionMajor type="Integer" value="1"/>
0574	<ProtocolVersionMinor type="Integer" value="2"/>
0575	</ProtocolVersion>
0576	<BatchCount type="Integer" value="1"/>
0577	</RequestHeader>
0578	<BatchItem>
0579	<Operation type="Enumeration" value="Destroy"/>
0580	<RequestPayload>
0581	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0582	</RequestPayload>
0583	</BatchItem>
0584	</RequestMessage>
0585	<ResponseMessage>
0586	<ResponseHeader>
0587	<ProtocolVersion>
0588	<ProtocolVersionMajor type="Integer" value="1"/>
0589	<ProtocolVersionMinor type="Integer" value="2"/>
0590	</ProtocolVersion>
0591	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0592	<BatchCount type="Integer" value="1"/>
0593	</ResponseHeader>
0594	<BatchItem>
0595	<Operation type="Enumeration" value="Destroy"/>
0596	<ResultStatus type="Enumeration" value="Success"/>
0597	<ResponsePayload>
0598	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0599	</ResponsePayload>
0600	</BatchItem>
0601	</ResponseMessage>
# TIME 12	
0602	<RequestMessage>
0603	<RequestHeader>
0604	<ProtocolVersion>
0605	<ProtocolVersionMajor type="Integer" value="1"/>
0606	<ProtocolVersionMinor type="Integer" value="2"/>
0607	</ProtocolVersion>
0608	<BatchCount type="Integer" value="1"/>
0609	</RequestHeader>
0610	<BatchItem>
0611	<Operation type="Enumeration" value="Destroy"/>
0612	<RequestPayload>
0613	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0614	</RequestPayload>
0615	</BatchItem>
0616	</RequestMessage>
0617	<ResponseMessage>
0618	<ResponseHeader>

0619	<ProtocolVersion>
0620	<ProtocolVersionMajor type="Integer" value="1"/>
0621	<ProtocolVersionMinor type="Integer" value="2"/>
0622	</ProtocolVersion>
0623	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0624	<BatchCount type="Integer" value="1"/>
0625	</ResponseHeader>
0626	<BatchItem>
0627	<Operation type="Enumeration" value="Destroy"/>
0628	<ResultStatus type="Enumeration" value="Success"/>
0629	<ResponsePayload>
0630	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0631	</ResponsePayload>
0632	</BatchItem>
0633	</ResponseMessage>
# TIME 13	
0634	<RequestMessage>
0635	<RequestHeader>
0636	<ProtocolVersion>
0637	<ProtocolVersionMajor type="Integer" value="1"/>
0638	<ProtocolVersionMinor type="Integer" value="2"/>
0639	</ProtocolVersion>
0640	<BatchCount type="Integer" value="1"/>
0641	</RequestHeader>
0642	<BatchItem>
0643	<Operation type="Enumeration" value="Destroy"/>
0644	<RequestPayload>
0645	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0646	</RequestPayload>
0647	</BatchItem>
0648	</RequestMessage>
0649	<ResponseMessage>
0650	<ResponseHeader>
0651	<ProtocolVersion>
0652	<ProtocolVersionMajor type="Integer" value="1"/>
0653	<ProtocolVersionMinor type="Integer" value="2"/>
0654	</ProtocolVersion>
0655	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0656	<BatchCount type="Integer" value="1"/>
0657	</ResponseHeader>
0658	<BatchItem>
0659	<Operation type="Enumeration" value="Destroy"/>
0660	<ResultStatus type="Enumeration" value="Success"/>
0661	<ResponsePayload>
0662	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0663	</ResponsePayload>
0664	</BatchItem>
0665	</ResponseMessage>

943

944 2.3.27 TC-134-12 - Register Key Pair, Certify and Re-certify Public Key

945 Register a public/private key pair on the server. Request the server to have a certificate created
946 using the Certify operation. Retrieve the certificate and its attributes, then execute the Re-
947 certify operation to re-certify the public key. Finally, destroy all the objects.

948 The new KMIP 1.1 certificate DN attributes are retrieved as are the original (deprecated) KMIP
949 1.0 certificate DN attributes.

```
# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="2"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="Register"/>
0011     <RequestPayload>
0012       <ObjectType type="Enumeration" value="PublicKey"/>
0013       <TemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0016           <AttributeValue type="Integer" value="Verify"/>
0017         </Attribute>
0018         <Attribute>
0019           <AttributeName type="TextString" value="x-ID"/>
0020           <AttributeValue type="TextString" value="TC-134-12-
pubkey1"/>
0021         </Attribute>
0022       </TemplateAttribute>
0023       <PublicKey>
0024         <KeyBlock>
0025           <KeyFormatType type="Enumeration" value="PKCS_1"/>
0026           <KeyValue>
0027             <KeyMaterial type="ByteString"
value="3082010a0282010100ab7f161c0042496ccd6c6d4dad9199734353577760
03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b
8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89
b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981
35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328
abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013
da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612
a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010
001"/>
0028           </KeyValue>
0029           <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0030           <CryptographicLength type="Integer" value="2048"/>
0031         </KeyBlock>
0032       </PublicKey>
0033     </RequestPayload>
0034   </BatchItem>
0035 </RequestMessage>
```


0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="2"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="2"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PrivateKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0068	<AttributeValue type="Integer" value="Sign"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>
0073	<LinkType type="Enumeration" value="PublicKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0075	</AttributeValue>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-134-12-
	prikey1"/>
0080	</Attribute>
0081	</TemplateAttribute>
0082	<PrivateKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString"
	value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353

	57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483 46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa 2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650 89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c 795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f 91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281 5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050 203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a 7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f a74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b 2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0 e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e 3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78 965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8 c3cdc2464744a793713dafb9f1dbcb799ff96423fecdd3cba794286bce920f4b5c183f 99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967 4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064 b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e 59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4 990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766 b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab 7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0 e94adlee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa elebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2 7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eae9a922fd75d5b16b1a5 61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a72 6a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171 666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520 a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a 1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d34941 7e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f812 9c32341a8b44f"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0089	<CryptographicLength type="Integer" value="2048"/>
0090	</KeyBlock>
0091	</PrivateKey>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="2"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString"

0109	value="\$UNIQUE_IDENTIFIER_1"/>
0110	</ResponsePayload>
0111	</BatchItem>
0112	</ResponseMessage>
# TIME 2	
0112	<RequestMessage>
0113	<RequestHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="2"/>
0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="AddAttribute"/>
0122	<RequestPayload>
0123	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Link"/>
0126	<AttributeValue>
0127	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0128	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0129	</AttributeValue>
0130	</Attribute>
0131	</RequestPayload>
0132	</BatchItem>
0133	</RequestMessage>
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="2"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="AddAttribute"/>
0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0148	<Attribute>
0149	<AttributeName type="TextString" value="Link"/>
0150	<AttributeValue>
0151	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0152	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0153	</AttributeValue>
0154	</Attribute>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
# TIME 3	

0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="2"/>
0163	</ProtocolVersion>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Certify"/>
0168	<RequestPayload>
0169	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0170	<CertificateRequestType type="Enumeration" value="PKCS_10"/>
0171	<CertificateRequest type="ByteString"
	value="3082028130820169020100303c310b3009060355040613025553310d300b0
	60355040a130441434d45310d300b060355040b13044b4d4950310f300d060355040
	31306436c69656e7430820122300d06092a864886f70d01010105000382010f00308
	2010a0282010100ab7f161c0042496ccd6c6d4dad919973435357776003acf54b7a
	f1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b8d71812b20
	5387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89b9bee9e60a
	1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f98135b1c67b70
	1675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328abf70e1b42
	e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da809e9c1b
	7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a29a82d73a
	1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010001a000300
	d06092a864886f70d010105050003820101002d90f5492c3df1771df4e87e1087cb9
	52197319a9696e2d588efda580d8d3304427b997cd921ad7c674aea413fba85fd61e
	6a481de9ab2e8a4ff43c02655015d3437f783fe0c781519cd08ffd3c007c7fade963
	2fe5659e2cac35bd6aaf3e13dc18097d996df01b66fc5e26ca109380863a209125cc
	0fd79533f327falcad444d89d3ff81b92a91428c469c846090fd1324846e12d01671
	962c332a7826152daaf486cc867185c2e27caf2f009898db07fe4b45c518192aa493
	d8f8c0198db67f90672ab6de05a08032941377f473d80716d85adc6182003ab34942
	302214eb3895f15403f2616adfd6bb5e6aa47fa38c9dfc73f4de80ddb91bdb04d21c
	82ba6"/>
0172	<TemplateAttribute>
0173	<Attribute>
0174	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0175	<AttributeValue type="Integer" value="Verify Sign"/>
0176	</Attribute>
0177	</Attribute>
0178	<AttributeName type="TextString" value="Name"/>
0179	<AttributeValue>
0180	<NameValue type="TextString" value="TC-134-12-
	certificatel"/>
0181	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0182	</AttributeValue>
0183	</Attribute>
0184	</TemplateAttribute>
0185	</RequestPayload>
0186	</BatchItem>
0187	</RequestMessage>
0188	<ResponseMessage>
0189	<ResponseHeader>
0190	<ProtocolVersion>

0191	<ProtocolVersionMajor type="Integer" value="1"/>
0192	<ProtocolVersionMinor type="Integer" value="2"/>
0193	</ProtocolVersion>
0194	<TimeStamp type="DateTime" value="2012-04-27T08:14:41+00:00"/>
0195	<BatchCount type="Integer" value="1"/>
0196	</ResponseHeader>
0197	<BatchItem>
0198	<Operation type="Enumeration" value="Certify"/>
0199	<ResultStatus type="Enumeration" value="Success"/>
0200	<ResponsePayload>
0201	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0202	</ResponsePayload>
0203	</BatchItem>
0204	</ResponseMessage>
# TIME 4	
0205	<RequestMessage>
0206	<RequestHeader>
0207	<ProtocolVersion>
0208	<ProtocolVersionMajor type="Integer" value="1"/>
0209	<ProtocolVersionMinor type="Integer" value="2"/>
0210	</ProtocolVersion>
0211	<BatchCount type="Integer" value="1"/>
0212	</RequestHeader>
0213	<BatchItem>
0214	<Operation type="Enumeration" value="Get"/>
0215	<RequestPayload>
0216	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0217	</RequestPayload>
0218	</BatchItem>
0219	</RequestMessage>
0220	<ResponseMessage>
0221	<ResponseHeader>
0222	<ProtocolVersion>
0223	<ProtocolVersionMajor type="Integer" value="1"/>
0224	<ProtocolVersionMinor type="Integer" value="2"/>
0225	</ProtocolVersion>
0226	<TimeStamp type="DateTime" value="2013-06-18T08:55:57+00:00"/>
0227	<BatchCount type="Integer" value="1"/>
0228	</ResponseHeader>
0229	<BatchItem>
0230	<Operation type="Enumeration" value="Get"/>
0231	<ResultStatus type="Enumeration" value="Success"/>
0232	<ResponsePayload>
0233	<ObjectType type="Enumeration" value="Certificate"/>
0234	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0235	<Certificate>
0236	<CertificateType type="Enumeration" value="X_509"/>
0237	<CertificateValue type="ByteString"
	value="30820277308201e0a0030201020209009bba23d1b6a48f97300d06092a864886f70d01010b0500303b310b3009060355040613025553310d300b060355040a130454455354310e300c060355040b13054f41534953310d300b060355040313044b4d4950301e170d3133303631383038353535375a170d3134303631383038353535375a303c310b3009060355040613025553310d300b060355040a130441434d45310d300b060355040b13044b4d4950310f300d06035504031306436c69656e7430820122300d0

0238	6092a864886f70d01010105000382010f003082010a0282010100ab7f161c0042496
0239	ccd6c6d4dadb919973435357776003acf54b7af1e440afb80b64a8755f8002cfeba6
0240	b184540a2d66086d74648346d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176
0241	b7957c422e7d03fc6267fa2a6f89b9bee9e60ald7c2d833e5a5f4bb0b1434f4e795a
	41100f8aa214900df8b65089f98135b1c67b701675abdbc7d5721aac9d14a7f081fc
	ec80b64e8a0ecc8295353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d2112
	6eba8da7d0ca34142cb76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c
	8d7cce8946a9ac99b1c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6f
	c411335d5dc7426b0f6050203010001300d06092a864886f70d01010b05000381810
	0c4fe08d5bd74239648c7faabaed0978527ac01a0fd17b8a65c0d92501c4eab3f487
	511062eafedc1024e74dc6bfdaae7f66d1fdda7574f6db3f03c6de83586b52c593a4
	671001a0531bc43eff4849880b07924b7a9a0236d5d64d82d4d8e42dcd3a72c80728
	804f9ba7f0e80c3fe3eb09cb3ed7fbfb2167c99be513ff9db0b6"/>
	</Certificate>
	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>
0242	# TIME 5
0243	<RequestMessage>
0244	<RequestHeader>
0245	<ProtocolVersion>
0246	<ProtocolVersionMajor type="Integer" value="1"/>
0247	<ProtocolVersionMinor type="Integer" value="2"/>
0248	</ProtocolVersion>
0249	<BatchCount type="Integer" value="1"/>
0250	</RequestHeader>
0251	<BatchItem>
0252	<Operation type="Enumeration" value="GetAttributeList"/>
0253	<RequestPayload>
0254	<UniqueIdentifier type="TextString"
0255	value="\$UNIQUE_IDENTIFIER_2"/>
0256	</RequestPayload>
0257	</BatchItem>
0258	</RequestMessage>
0259	<ResponseMessage>
0260	<ResponseHeader>
0261	<ProtocolVersion>
0262	<ProtocolVersionMajor type="Integer" value="1"/>
0263	<ProtocolVersionMinor type="Integer" value="2"/>
0264	</ProtocolVersion>
0265	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0266	<BatchCount type="Integer" value="1"/>
0267	</ResponseHeader>
0268	<BatchItem>
0269	<Operation type="Enumeration" value="GetAttributeList"/>
0270	<ResultStatus type="Enumeration" value="Success"/>
0271	<ResponsePayload>
0272	<UniqueIdentifier type="TextString"
0273	value="\$UNIQUE_IDENTIFIER_2"/>
0274	<AttributeName type="TextString" value="Unique Identifier"/>
0275	<AttributeName type="TextString" value="Object Type"/>
0276	<AttributeName type="TextString" value="Certificate Type"/>
0277	<AttributeName type="TextString" value="Certificate Identifier"/>
	<AttributeName type="TextString" value="Certificate Issuer"/>
	<AttributeName type="TextString" value="Certificate Length"/>
	<AttributeName type="TextString" value="Certificate Subject"/>

0278	<AttributeName type="TextString" value="Cryptographic
0279	Length"/>
0279	<AttributeName type="TextString" value="Cryptographic Usage
0280	Mask"/>
0280	<AttributeName type="TextString" value="Digest"/>
0281	<AttributeName type="TextString" value="Digital Signature
0282	Algorithm"/>
0282	<AttributeName type="TextString" value="Fresh"/>
0283	<AttributeName type="TextString" value="Initial Date"/>
0284	<AttributeName type="TextString" value="Last Change Date"/>
0285	<AttributeName type="TextString" value="Lease Time"/>
0286	<AttributeName type="TextString" value="Link"/>
0287	<AttributeName type="TextString" value="Name"/>
0288	<AttributeName type="TextString" value="Original Creation
0289	Date"/>
0289	<AttributeName type="TextString" value="State"/>
0290	<AttributeName type="TextString" value="X.509 Certificate
0291	Identifier"/>
0291	<AttributeName type="TextString" value="X.509 Certificate
0292	Issuer"/>
0292	<AttributeName type="TextString" value="X.509 Certificate
0293	Subject"/>
0293	</ResponsePayload>
0294	</BatchItem>
0295	</ResponseMessage>
# TIME 6	
0296	<RequestMessage>
0297	<RequestHeader>
0298	<ProtocolVersion>
0299	<ProtocolVersionMajor type="Integer" value="1"/>
0300	<ProtocolVersionMinor type="Integer" value="2"/>
0301	</ProtocolVersion>
0302	<BatchCount type="Integer" value="1"/>
0303	</RequestHeader>
0304	<BatchItem>
0305	<Operation type="Enumeration" value="GetAttributes"/>
0306	<RequestPayload>
0307	<UniqueIdentifier type="TextString"
0308	value="\$UNIQUE_IDENTIFIER_2"/>
0308	<AttributeName type="TextString" value="Certificate
0309	Identifier"/>
0309	<AttributeName type="TextString" value="Certificate Issuer"/>
0310	<AttributeName type="TextString" value="Certificate Subject"/>
0311	<AttributeName type="TextString" value="Certificate Type"/>
0312	<AttributeName type="TextString" value="Digital Signature
0313	Algorithm"/>
0313	<AttributeName type="TextString" value="Cryptographic
0314	Length"/>
0314	<AttributeName type="TextString" value="Certificate Length"/>
0315	<AttributeName type="TextString" value="X.509 Certificate
0316	Identifier"/>
0316	<AttributeName type="TextString" value="X.509 Certificate
0317	Issuer"/>
0317	<AttributeName type="TextString" value="X.509 Certificate
0318	Subject"/>
0318	</RequestPayload>
0319	</BatchItem>

0320	</RequestMessage>
0321	<ResponseMessage>
0322	<ResponseHeader>
0323	<ProtocolVersion>
0324	<ProtocolVersionMajor type="Integer" value="1"/>
0325	<ProtocolVersionMinor type="Integer" value="2"/>
0326	</ProtocolVersion>
0327	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0328	<BatchCount type="Integer" value="1"/>
0329	</ResponseHeader>
0330	<BatchItem>
0331	<Operation type="Enumeration" value="GetAttributes"/>
0332	<ResultStatus type="Enumeration" value="Success"/>
0333	<ResponsePayload>
0334	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0335	<Attribute>
0336	<AttributeName type="TextString" value="Certificate"
	Identifier"/>
0337	<AttributeValue>
0338	<Issuer type="TextString"
	value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0339	<SerialNumber type="TextString" value="9BBA23D1B6A48F97"/>
0340	</AttributeValue>
0341	</Attribute>
0342	<Attribute>
0343	<AttributeName type="TextString" value="Certificate"
	Issuer"/>
0344	<AttributeValue>
0345	<CertificateIssuerDistinguishedName type="TextString"
	value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0346	</AttributeValue>
0347	</Attribute>
0348	<Attribute>
0349	<AttributeName type="TextString" value="Certificate"
	Subject"/>
0350	<AttributeValue>
0351	<CertificateSubjectDistinguishedName type="TextString"
	value="CN=Client,OU=KMIP,O=ACME,C=US"/>
0352	</AttributeValue>
0353	</Attribute>
0354	<Attribute>
0355	<AttributeName type="TextString" value="Certificate Type"/>
0356	<AttributeValue type="Enumeration" value="X_509"/>
0357	</Attribute>
0358	<Attribute>
0359	<AttributeName type="TextString" value="Digital Signature"
	Algorithm"/>
0360	<AttributeValue type="Enumeration"
	value="SHA_256WithRSAEncryption"/>
0361	</Attribute>
0362	<Attribute>
0363	<AttributeName type="TextString" value="Cryptographic"
	Length"/>
0364	<AttributeValue type="Integer" value="2048"/>
0365	</Attribute>
0366	</Attribute>

0367	<AttributeName type="TextString" value="Certificate
0368	Length"/>
0369	<AttributeValue type="Integer" value="635"/>
0370	</Attribute>
0371	<AttributeName type="TextString" value="X.509 Certificate
0372	Identifier"/>
0373	<AttributeValue>
0374	<IssuerDistinguishedName type="ByteString"
0375	value="303b310b3009060355040613025553310d300b060355040a1304544553543
0376	10e300c060355040b13054f41534953310d300b060355040313044b4d4950"/>
0377	<CertificateSerialNumber type="ByteString"
0378	value="0209009bba23d1b6a48f97"/>
0379	</AttributeValue>
0380	</Attribute>
0381	<AttributeName type="TextString" value="X.509 Certificate
0382	Issuer"/>
0383	<AttributeValue>
0384	<IssuerDistinguishedName type="ByteString"
0385	value="303b310b3009060355040613025553310d300b060355040a1304544553543
0386	10e300c060355040b13054f41534953310d300b060355040313044b4d4950"/>
0387	</AttributeValue>
0388	</Attribute>
0389	<Attribute>
0390	<AttributeName type="TextString" value="X.509 Certificate
0391	Subject"/>
0392	<AttributeValue>
0393	<SubjectDistinguishedName type="ByteString"
0394	value="303c310b3009060355040613025553310d300b060355040a130441434d453
0395	10d300b060355040b13044b4d4950310f300d06035504031306436c69656e74"/>
0396	</AttributeValue>
0397	</Attribute>
0398	</ResponsePayload>
0399	</BatchItem>
0400	</ResponseMessage>
0401	# TIME 7
0402	<RequestMessage>
0403	<RequestHeader>
0404	<ProtocolVersion>
0405	<ProtocolVersionMajor type="Integer" value="1"/>
0406	<ProtocolVersionMinor type="Integer" value="2"/>
0407	</ProtocolVersion>
0408	<BatchCount type="Integer" value="1"/>
0409	</RequestHeader>
0410	<BatchItem>
0411	<Operation type="Enumeration" value="ReCertify"/>
0412	<RequestPayload>
0413	<UniqueIdentifier type="TextString"
0414	value="\$UNIQUE_IDENTIFIER_2"/>
0415	<CertificateRequestType type="Enumeration" value="PKCS_10"/>
0416	<CertificateRequest type="ByteString"
0417	value="3082028130820169020100303c310b3009060355040613025553310d300b0
0418	60355040a130441434d45310d300b060355040b13044b4d4950310f300d060355040
0419	31306436c69656e7430820122300d06092a864886f70d01010105000382010f00308
0420	2010a0282010100ab7f161c0042496ccd6c6d4dadb919973435357776003acf54b7a
0421	f1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b8d71812b20

	5387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f98135b1c67b701675abdbbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010001a000300d06092a864886f70d010105050003820101002d90f5492c3df1771df4e87e1087cb952197319a9696e2d588efda580d8d3304427b997cd921ad7c674aea413fba85fd61e6a481de9ab2e8a4ff43c02655015d3437f783fe0c781519cd08ffd3c007c7fade9632fe5659e2cac35bd6aaf3e13dc18097d996df01b66fc5e26ca109380863a209125cc0fd79533f327falcad444d89d3ff81b92a91428c469c846090fd1324846e12d01671962c332a7826152daaf486cc867185c2e27caf2f009898db07fe4b45c518192aa493d8f8c0198db67f90672ab6de05a08032941377f473d80716d85adc6182003ab34942302214eb3895f15403f2616adfd6bb5e6aa47fa38c9dfc73f4de80ddb91bdb04d21c82ba6"/>
0406	<TemplateAttribute>
0407	<Attribute>
0408	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0409	<AttributeValue type="Integer" value="Verify Sign"/>
0410	</Attribute>
0411	<Attribute>
0412	<AttributeName type="TextString" value="Name"/>
0413	<AttributeValue>
0414	<NameValue type="TextString" value="TC-134-12-certificate2"/>
0415	<NameType type="Enumeration" value="UninterpretedTextString"/>
0416	</AttributeValue>
0417	</Attribute>
0418	</TemplateAttribute>
0419	</RequestPayload>
0420	</BatchItem>
0421	</RequestMessage>
0422	<ResponseMessage>
0423	<ResponseHeader>
0424	<ProtocolVersion>
0425	<ProtocolVersionMajor type="Integer" value="1"/>
0426	<ProtocolVersionMinor type="Integer" value="2"/>
0427	</ProtocolVersion>
0428	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0429	<BatchCount type="Integer" value="1"/>
0430	</ResponseHeader>
0431	<BatchItem>
0432	<Operation type="Enumeration" value="ReCertify"/>
0433	<ResultStatus type="Enumeration" value="Success"/>
0434	<ResponsePayload>
0435	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_3"/>
0436	</ResponsePayload>
0437	</BatchItem>
0438	</ResponseMessage>
	# TIME 8
0439	<RequestMessage>
0440	<RequestHeader>
0441	<ProtocolVersion>
0442	<ProtocolVersionMajor type="Integer" value="1"/>

0443	<ProtocolVersionMinor type="Integer" value="2"/>
0444	</ProtocolVersion>
0445	<BatchCount type="Integer" value="1"/>
0446	</RequestHeader>
0447	<BatchItem>
0448	<Operation type="Enumeration" value="GetAttributes"/>
0449	<RequestPayload>
0450	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0451	<AttributeName type="TextString" value="Link"/>
0452	</RequestPayload>
0453	</BatchItem>
0454	</RequestMessage>
0455	<ResponseMessage>
0456	<ResponseHeader>
0457	<ProtocolVersion>
0458	<ProtocolVersionMajor type="Integer" value="1"/>
0459	<ProtocolVersionMinor type="Integer" value="2"/>
0460	</ProtocolVersion>
0461	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0462	<BatchCount type="Integer" value="1"/>
0463	</ResponseHeader>
0464	<BatchItem>
0465	<Operation type="Enumeration" value="GetAttributes"/>
0466	<ResultStatus type="Enumeration" value="Success"/>
0467	<ResponsePayload>
0468	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0469	<Attribute>
0470	<AttributeName type="TextString" value="Link"/>
0471	<AttributeValue>
0472	<LinkType type="Enumeration" value="PublicKeyLink"/>
0473	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0474	</AttributeValue>
0475	</Attribute>
0476	</ResponsePayload>
0477	</BatchItem>
0478	</ResponseMessage>
	# TIME 9
0479	<RequestMessage>
0480	<RequestHeader>
0481	<ProtocolVersion>
0482	<ProtocolVersionMajor type="Integer" value="1"/>
0483	<ProtocolVersionMinor type="Integer" value="2"/>
0484	</ProtocolVersion>
0485	<BatchCount type="Integer" value="1"/>
0486	</RequestHeader>
0487	<BatchItem>
0488	<Operation type="Enumeration" value="GetAttributes"/>
0489	<RequestPayload>
0490	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0491	<AttributeName type="TextString" value="Link"/>
0492	</RequestPayload>
0493	</BatchItem>
0494	</RequestMessage>

0495	<ResponseMessage>
0496	<ResponseHeader>
0497	<ProtocolVersion>
0498	<ProtocolVersionMajor type="Integer" value="1"/>
0499	<ProtocolVersionMinor type="Integer" value="2"/>
0500	</ProtocolVersion>
0501	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0502	<BatchCount type="Integer" value="1"/>
0503	</ResponseHeader>
0504	<BatchItem>
0505	<Operation type="Enumeration" value="GetAttributes"/>
0506	<ResultStatus type="Enumeration" value="Success"/>
0507	<ResponsePayload>
0508	<UniqueIdentifier type="TextString"
0509	value="\$UNIQUE_IDENTIFIER_0"/>
0510	<Attribute>
0511	<AttributeName type="TextString" value="Link"/>
0512	<AttributeValue>
0513	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0514	<LinkedObjectIdentifier type="TextString"
0515	value="\$UNIQUE_IDENTIFIER_1"/>
0516	</AttributeValue>
0517	</Attribute>
0518	<Attribute>
0519	<AttributeName type="TextString" value="Link"/>
0520	<AttributeIndex type="Integer" value="1"/>
0521	<AttributeValue>
0522	<LinkType type="Enumeration" value="CertificateLink"/>
0523	<LinkedObjectIdentifier type="TextString"
0524	value="\$UNIQUE_IDENTIFIER_3"/>
0525	</AttributeValue>
0526	</Attribute>
0527	</ResponsePayload>
0528	</BatchItem>
0529	</ResponseMessage>
0530	# TIME 10
0531	<RequestMessage>
0532	<RequestHeader>
0533	<ProtocolVersion>
0534	<ProtocolVersionMajor type="Integer" value="1"/>
0535	<ProtocolVersionMinor type="Integer" value="2"/>
0536	</ProtocolVersion>
0537	<BatchCount type="Integer" value="1"/>
0538	</RequestHeader>
0539	<BatchItem>
0540	<Operation type="Enumeration" value="GetAttributes"/>
0541	<RequestPayload>
0542	<UniqueIdentifier type="TextString"
0543	value="\$UNIQUE_IDENTIFIER_2"/>
0544	<AttributeName type="TextString" value="Link"/>
0545	</RequestPayload>
0546	</BatchItem>
	</RequestMessage>
	<ResponseMessage>
	<ResponseHeader>
	<ProtocolVersion>
	<ProtocolVersionMajor type="Integer" value="1"/>

0547	<ProtocolVersionMinor type="Integer" value="2"/>
0548	</ProtocolVersion>
0549	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0550	<BatchCount type="Integer" value="1"/>
0551	</ResponseHeader>
0552	<BatchItem>
0553	<Operation type="Enumeration" value="GetAttributes"/>
0554	<ResultStatus type="Enumeration" value="Success"/>
0555	<ResponsePayload>
0556	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0557	<Attribute>
0558	<AttributeName type="TextString" value="Link"/>
0559	<AttributeValue>
0560	<LinkType type="Enumeration" value="PublicKeyLink"/>
0561	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0562	</AttributeValue>
0563	</Attribute>
0564	<Attribute>
0565	<AttributeName type="TextString" value="Link"/>
0566	<AttributeIndex type="Integer" value="1"/>
0567	<AttributeValue>
0568	<LinkType type="Enumeration"
	value="ReplacementObjectLink"/>
0569	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0570	</AttributeValue>
0571	</Attribute>
0572	</ResponsePayload>
0573	</BatchItem>
0574	</ResponseMessage>
# TIME 11	
0575	<RequestMessage>
0576	<RequestHeader>
0577	<ProtocolVersion>
0578	<ProtocolVersionMajor type="Integer" value="1"/>
0579	<ProtocolVersionMinor type="Integer" value="2"/>
0580	</ProtocolVersion>
0581	<BatchCount type="Integer" value="1"/>
0582	</RequestHeader>
0583	<BatchItem>
0584	<Operation type="Enumeration" value="GetAttributes"/>
0585	<RequestPayload>
0586	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0587	<AttributeName type="TextString" value="Link"/>
0588	<AttributeName type="TextString" value="Certificate
	Identifier"/>
0589	<AttributeName type="TextString" value="Name"/>
0590	</RequestPayload>
0591	</BatchItem>
0592	</RequestMessage>
0593	<ResponseMessage>
0594	<ResponseHeader>
0595	<ProtocolVersion>
0596	<ProtocolVersionMajor type="Integer" value="1"/>

```

0597     <ProtocolVersionMinor type="Integer" value="2"/>
0598     </ProtocolVersion>
0599     <TimeStamp type="DateTime" value="2013-06-18T08:55:57+00:00"/>
0600     <BatchCount type="Integer" value="1"/>
0601 </ResponseHeader>
0602 <BatchItem>
0603     <Operation type="Enumeration" value="GetAttributes"/>
0604     <ResultStatus type="Enumeration" value="Success"/>
0605     <ResponsePayload>
0606         <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_3"/>
0607         <Attribute>
0608             <AttributeName type="TextString" value="Link"/>
0609             <AttributeValue>
0610                 <LinkType type="Enumeration" value="PublicKeyLink"/>
0611                 <LinkedObjectIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0612             </AttributeValue>
0613         </Attribute>
0614         <Attribute>
0615             <AttributeName type="TextString" value="Link"/>
0616             <AttributeIndex type="Integer" value="1"/>
0617             <AttributeValue>
0618                 <LinkType type="Enumeration" value="ReplacedObjectLink"/>
0619                 <LinkedObjectIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_2"/>
0620             </AttributeValue>
0621         </Attribute>
0622         <Attribute>
0623             <AttributeName type="TextString" value="Certificate
Identifier"/>
0624             <AttributeValue>
0625                 <Issuer type="TextString"
value="CN=KMIP,OU=OASIS,O=TEST,C=US"/>
0626                 <SerialNumber type="TextString" value="CF77F7A23282BC12"/>
0627             </AttributeValue>
0628         </Attribute>
0629         <Attribute>
0630             <AttributeName type="TextString" value="Name"/>
0631             <AttributeValue>
0632                 <NameValue type="TextString" value="TC-134-12-
certificate2"/>
0633                 <NameType type="Enumeration"
value="UninterpretedTextString"/>
0634             </AttributeValue>
0635         </Attribute>
0636         <Attribute>
0637             <AttributeName type="TextString" value="Name"/>
0638             <AttributeIndex type="Integer" value="1"/>
0639             <AttributeValue>
0640                 <NameValue type="TextString" value="TC-134-12-
certificate1"/>
0641                 <NameType type="Enumeration"
value="UninterpretedTextString"/>
0642             </AttributeValue>
0643         </Attribute>
0644     </ResponsePayload>

```

0645	</BatchItem>
0646	</ResponseMessage>
# TIME 12	
0647	<RequestMessage>
0648	<RequestHeader>
0649	<ProtocolVersion>
0650	<ProtocolVersionMajor type="Integer" value="1"/>
0651	<ProtocolVersionMinor type="Integer" value="2"/>
0652	</ProtocolVersion>
0653	<BatchCount type="Integer" value="1"/>
0654	</RequestHeader>
0655	<BatchItem>
0656	<Operation type="Enumeration" value="Destroy"/>
0657	<RequestPayload>
0658	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0659	</RequestPayload>
0660	</BatchItem>
0661	</RequestMessage>
0662	<ResponseMessage>
0663	<ResponseHeader>
0664	<ProtocolVersion>
0665	<ProtocolVersionMajor type="Integer" value="1"/>
0666	<ProtocolVersionMinor type="Integer" value="2"/>
0667	</ProtocolVersion>
0668	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0669	<BatchCount type="Integer" value="1"/>
0670	</ResponseHeader>
0671	<BatchItem>
0672	<Operation type="Enumeration" value="Destroy"/>
0673	<ResultStatus type="Enumeration" value="Success"/>
0674	<ResponsePayload>
0675	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0676	</ResponsePayload>
0677	</BatchItem>
0678	</ResponseMessage>
# TIME 13	
0679	<RequestMessage>
0680	<RequestHeader>
0681	<ProtocolVersion>
0682	<ProtocolVersionMajor type="Integer" value="1"/>
0683	<ProtocolVersionMinor type="Integer" value="2"/>
0684	</ProtocolVersion>
0685	<BatchCount type="Integer" value="1"/>
0686	</RequestHeader>
0687	<BatchItem>
0688	<Operation type="Enumeration" value="Destroy"/>
0689	<RequestPayload>
0690	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0691	</RequestPayload>
0692	</BatchItem>
0693	</RequestMessage>
0694	<ResponseMessage>
0695	<ResponseHeader>

0696	<ProtocolVersion>
0697	<ProtocolVersionMajor type="Integer" value="1"/>
0698	<ProtocolVersionMinor type="Integer" value="2"/>
0699	</ProtocolVersion>
0700	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0701	<BatchCount type="Integer" value="1"/>
0702	</ResponseHeader>
0703	<BatchItem>
0704	<Operation type="Enumeration" value="Destroy"/>
0705	<ResultStatus type="Enumeration" value="Success"/>
0706	<ResponsePayload>
0707	<UniqueIdentifier type="TextString"
0708	value="\$UNIQUE_IDENTIFIER_0"/>
0709	</ResponsePayload>
0710	</BatchItem>
0711	</ResponseMessage>
# TIME 14	
0711	<RequestMessage>
0712	<RequestHeader>
0713	<ProtocolVersion>
0714	<ProtocolVersionMajor type="Integer" value="1"/>
0715	<ProtocolVersionMinor type="Integer" value="2"/>
0716	</ProtocolVersion>
0717	<BatchCount type="Integer" value="1"/>
0718	</RequestHeader>
0719	<BatchItem>
0720	<Operation type="Enumeration" value="Destroy"/>
0721	<RequestPayload>
0722	<UniqueIdentifier type="TextString"
0723	value="\$UNIQUE_IDENTIFIER_2"/>
0724	</RequestPayload>
0725	</BatchItem>
0726	</RequestMessage>
0727	<ResponseMessage>
0728	<ResponseHeader>
0729	<ProtocolVersion>
0730	<ProtocolVersionMajor type="Integer" value="1"/>
0731	<ProtocolVersionMinor type="Integer" value="2"/>
0732	</ProtocolVersion>
0733	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0734	<BatchCount type="Integer" value="1"/>
0735	</ResponseHeader>
0736	<BatchItem>
0737	<Operation type="Enumeration" value="Destroy"/>
0738	<ResultStatus type="Enumeration" value="Success"/>
0739	<ResponsePayload>
0740	<UniqueIdentifier type="TextString"
0741	value="\$UNIQUE_IDENTIFIER_2"/>
0742	</ResponsePayload>
0743	</BatchItem>
0744	</ResponseMessage>
# TIME 15	
0743	<RequestMessage>
0744	<RequestHeader>
0745	<ProtocolVersion>
0746	<ProtocolVersionMajor type="Integer" value="1"/>

0747	<ProtocolVersionMinor type="Integer" value="2"/>
0748	</ProtocolVersion>
0749	<BatchCount type="Integer" value="1"/>
0750	</RequestHeader>
0751	<BatchItem>
0752	<Operation type="Enumeration" value="Destroy"/>
0753	<RequestPayload>
0754	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0755	</RequestPayload>
0756	</BatchItem>
0757	</RequestMessage>
0758	<ResponseMessage>
0759	<ResponseHeader>
0760	<ProtocolVersion>
0761	<ProtocolVersionMajor type="Integer" value="1"/>
0762	<ProtocolVersionMinor type="Integer" value="2"/>
0763	</ProtocolVersion>
0764	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0765	<BatchCount type="Integer" value="1"/>
0766	</ResponseHeader>
0767	<BatchItem>
0768	<Operation type="Enumeration" value="Destroy"/>
0769	<ResultStatus type="Enumeration" value="Success"/>
0770	<ResponsePayload>
0771	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0772	</ResponsePayload>
0773	</BatchItem>
0774	</ResponseMessage>

950

951 2.3.28 TC-141-12 - Key Wrapping using AES Key Wrap and No Encoding

952 Register a 128-bit AES key encryption key (KEK) with the Cryptographic Usage Mask attribute set
953 to Wrap and the Cryptographic Parameters specifying NIST Key Wrap as the Block Cipher Mode.
954 Subsequently, register another 128-bit AES data key (DEK). Retrieve the data key wrapped using
955 the NIST Key Wrap algorithm and the KEK. The Encoding Option is set to No Encoding, which
956 means that only the key material is wrapped as opposed to the whole TTLV-encoded Key Value
957 structure being wrapped. Finally, destroy both keys to return the server to the initial state. The
958 key material for both the KEK and the DEK are from the test vectors specified in Section 4.6 of
959 [NISTKeyWrap].

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>

0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Name"/>
0016	<AttributeValue>
0017	<NameValue type="TextString" value="TC-141-12-key1"/>
0018	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0019	</AttributeValue>
0020	</Attribute>
0021	<Attribute>
0022	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0023	<AttributeValue type="Integer" value="WrapKey"/>
0024	</Attribute>
0025	<Attribute>
0026	<AttributeName type="TextString" value="Cryptographic
	Parameters"/>
0027	<AttributeValue>
0028	<BlockCipherMode type="Enumeration"
	value="NISTKeyWrap"/>
0029	</AttributeValue>
0030	</Attribute>
0031	<Attribute>
0032	<AttributeName type="TextString" value="Activation Date"/>
0033	<AttributeValue type="DateTime" value="\$NOW-3600"/>
0034	</Attribute>
0035	</TemplateAttribute>
0036	<SymmetricKey>
0037	<KeyBlock>
0038	<KeyFormatType type="Enumeration" value="Raw"/>
0039	<KeyValue>
0040	<KeyMaterial type="ByteString"
	value="000102030405060708090a0b0c0d0e0f"/>
0041	</KeyValue>
0042	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0043	<CryptographicLength type="Integer" value="128"/>
0044	</KeyBlock>
0045	</SymmetricKey>
0046	</RequestPayload>
0047	</BatchItem>
0048	</RequestMessage>
0049	<ResponseMessage>
0050	<ResponseHeader>
0051	<ProtocolVersion>
0052	<ProtocolVersionMajor type="Integer" value="1"/>
0053	<ProtocolVersionMinor type="Integer" value="2"/>
0054	</ProtocolVersion>
0055	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0056	<BatchCount type="Integer" value="1"/>
0057	</ResponseHeader>
0058	<BatchItem>
0059	<Operation type="Enumeration" value="Register"/>
0060	<ResultStatus type="Enumeration" value="Success"/>
0061	<ResponsePayload>
0062	<UniqueIdentifier type="TextString"

0063	value="\$UNIQUE_IDENTIFIER_0"/>
0064	</ResponsePayload>
0065	</BatchItem>
	</ResponseMessage>
0066	# TIME 1
0067	<RequestMessage>
0068	<RequestHeader>
0069	<ProtocolVersion>
0070	<ProtocolVersionMajor type="Integer" value="1"/>
0071	<ProtocolVersionMinor type="Integer" value="2"/>
0072	</ProtocolVersion>
0073	<BatchCount type="Integer" value="1"/>
0074	</RequestHeader>
0075	<BatchItem>
0076	<Operation type="Enumeration" value="Register"/>
0077	<RequestPayload>
0078	<ObjectType type="Enumeration" value="SymmetricKey"/>
0079	<TemplateAttribute>
0080	<Attribute>
0081	<AttributeName type="TextString" value="Name"/>
0082	<AttributeValue>
0083	<NameValue type="TextString" value="TC-141-12-key2"/>
0084	<NameType type="Enumeration"
0085	value="UninterpretedTextString"/>
0086	</AttributeValue>
0087	</Attribute>
0088	<Attribute type="TextString" value="Cryptographic
0089	Usage Mask"/>
0090	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0091	</Attribute>
0092	</TemplateAttribute>
0093	<SymmetricKey>
0094	<KeyBlock>
0095	<KeyFormatType type="Enumeration" value="Raw"/>
0096	<KeyMaterial type="ByteString"
0097	value="00112233445566778899aabbccddeeff"/>
0098	</KeyMaterial>
0099	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0100	<CryptographicLength type="Integer" value="128"/>
0101	</CryptographicAlgorithm>
0102	</KeyBlock>
0103	</SymmetricKey>
0104	</RequestPayload>
0105	</BatchItem>
0106	</RequestMessage>
0107	<ResponseMessage>
0108	<ResponseHeader>
0109	<ProtocolVersion>
0110	<ProtocolVersionMajor type="Integer" value="1"/>
0111	<ProtocolVersionMinor type="Integer" value="2"/>
0112	</ProtocolVersion>
0113	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0114	<BatchCount type="Integer" value="1"/>
	</ResponseHeader>
	<BatchItem>
	<Operation type="Enumeration" value="Register"/>

0115	<ResultStatus type="Enumeration" value="Success"/>
0116	<ResponsePayload>
0117	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0118	</ResponsePayload>
0119	</BatchItem>
0120	</ResponseMessage>
# TIME 2	
0121	<RequestMessage>
0122	<RequestHeader>
0123	<ProtocolVersion>
0124	<ProtocolVersionMajor type="Integer" value="1"/>
0125	<ProtocolVersionMinor type="Integer" value="2"/>
0126	</ProtocolVersion>
0127	<BatchCount type="Integer" value="1"/>
0128	</RequestHeader>
0129	<BatchItem>
0130	<Operation type="Enumeration" value="Get"/>
0131	<RequestPayload>
0132	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0133	<KeyWrappingSpecification>
0134	<WrappingMethod type="Enumeration" value="Encrypt"/>
0135	<EncryptionKeyInformation>
0136	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0137	<CryptographicParameters>
0138	<BlockCipherMode type="Enumeration"
	value="NISTKeyWrap"/>
0139	</CryptographicParameters>
0140	</EncryptionKeyInformation>
0141	<EncodingOption type="Enumeration" value="NoEncoding"/>
0142	</KeyWrappingSpecification>
0143	</RequestPayload>
0144	</BatchItem>
0145	</RequestMessage>
0146	<ResponseMessage>
0147	<ResponseHeader>
0148	<ProtocolVersion>
0149	<ProtocolVersionMajor type="Integer" value="1"/>
0150	<ProtocolVersionMinor type="Integer" value="2"/>
0151	</ProtocolVersion>
0152	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0153	<BatchCount type="Integer" value="1"/>
0154	</ResponseHeader>
0155	<BatchItem>
0156	<Operation type="Enumeration" value="Get"/>
0157	<ResultStatus type="Enumeration" value="Success"/>
0158	<ResponsePayload>
0159	<ObjectType type="Enumeration" value="SymmetricKey"/>
0160	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0161	<SymmetricKey>
0162	<KeyBlock>
0163	<KeyFormatType type="Enumeration" value="Raw"/>
0164	<KeyValue type="ByteString"
	value="1fa68b0a8112b447aef34bd8fb5a7b829d3e862371d2cfe5"/>

0165	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0166	<CryptographicLength type="Integer" value="128"/>
0167	<KeyWrappingData>
0168	<WrappingMethod type="Enumeration" value="Encrypt"/>
0169	<EncryptionKeyInformation>
0170	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0171	<CryptographicParameters>
0172	<BlockCipherMode type="Enumeration"
	value="NISTKeyWrap"/>
0173	</CryptographicParameters>
0174	</EncryptionKeyInformation>
0175	<EncodingOption type="Enumeration" value="NoEncoding"/>
0176	</KeyWrappingData>
0177	</KeyBlock>
0178	</SymmetricKey>
0179	</ResponsePayload>
0180	</BatchItem>
0181	</ResponseMessage>
	# TIME 3
0182	<RequestMessage>
0183	<RequestHeader>
0184	<ProtocolVersion>
0185	<ProtocolVersionMajor type="Integer" value="1"/>
0186	<ProtocolVersionMinor type="Integer" value="2"/>
0187	</ProtocolVersion>
0188	<BatchCount type="Integer" value="1"/>
0189	</RequestHeader>
0190	<BatchItem>
0191	<Operation type="Enumeration" value="Get"/>
0192	<RequestPayload>
0193	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0194	</RequestPayload>
0195	</BatchItem>
0196	</RequestMessage>
0197	<ResponseMessage>
0198	<ResponseHeader>
0199	<ProtocolVersion>
0200	<ProtocolVersionMajor type="Integer" value="1"/>
0201	<ProtocolVersionMinor type="Integer" value="2"/>
0202	</ProtocolVersion>
0203	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0204	<BatchCount type="Integer" value="1"/>
0205	</ResponseHeader>
0206	<BatchItem>
0207	<Operation type="Enumeration" value="Get"/>
0208	<ResultStatus type="Enumeration" value="Success"/>
0209	<ResponsePayload>
0210	<ObjectType type="Enumeration" value="SymmetricKey"/>
0211	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0212	<SymmetricKey>
0213	<KeyBlock>
0214	<KeyFormatType type="Enumeration" value="Raw"/>
0215	<KeyValue>
0216	<KeyMaterial type="ByteString"

0217	value="00112233445566778899aabbccddeeff"/>
0218	</KeyValue>
0219	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0220	<CryptographicLength type="Integer" value="128"/>
0221	</KeyBlock>
0222	</SymmetricKey>
0223	</ResponsePayload>
0224	</BatchItem>
0225	</ResponseMessage>
0226	# TIME 4
0227	<RequestMessage>
0228	<RequestHeader>
0229	<ProtocolVersion>
0230	<ProtocolVersionMajor type="Integer" value="1"/>
0231	<ProtocolVersionMinor type="Integer" value="2"/>
0232	</ProtocolVersion>
0233	<BatchCount type="Integer" value="1"/>
0234	</RequestHeader>
0235	<BatchItem>
0236	<Operation type="Enumeration" value="Destroy"/>
0237	<RequestPayload>
0238	<UniqueIdentifier type="TextString"
0239	value="\$UNIQUE_IDENTIFIER_1"/>
0240	</RequestPayload>
0241	</BatchItem>
0242	</RequestMessage>
0243	<ResponseMessage>
0244	<ResponseHeader>
0245	<ProtocolVersion>
0246	<ProtocolVersionMajor type="Integer" value="1"/>
0247	<ProtocolVersionMinor type="Integer" value="2"/>
0248	</ProtocolVersion>
0249	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0250	<BatchCount type="Integer" value="1"/>
0251	</ResponseHeader>
0252	<BatchItem>
0253	<Operation type="Enumeration" value="Destroy"/>
0254	<ResultStatus type="Enumeration" value="Success"/>
0255	<ResponsePayload>
0256	<UniqueIdentifier type="TextString"
0257	value="\$UNIQUE_IDENTIFIER_1"/>
0258	</ResponsePayload>
0259	</BatchItem>
0260	</ResponseMessage>
0261	# TIME 5
0262	<RequestMessage>
0263	<RequestHeader>
0264	<ProtocolVersion>
0265	<ProtocolVersionMajor type="Integer" value="1"/>
0266	<ProtocolVersionMinor type="Integer" value="2"/>
0267	</ProtocolVersion>
	<BatchCount type="Integer" value="1"/>
	</RequestHeader>
	<BatchItem>
	<Operation type="Enumeration" value="Revoke"/>
	<RequestPayload>

0268	<UniqueIdentifier type="TextString"
0269	value="\$UNIQUE_IDENTIFIER_0"/>
0270	<RevocationReason>
0271	<RevocationReasonCode type="Enumeration"
0272	value="Unspecified"/>
0273	</RevocationReason>
0274	</RequestPayload>
0275	</BatchItem>
0276	</RequestMessage>
0277	<ResponseMessage>
0278	<ResponseHeader>
0279	<ProtocolVersion>
0280	<ProtocolVersionMajor type="Integer" value="1"/>
0281	<ProtocolVersionMinor type="Integer" value="2"/>
0282	</ProtocolVersion>
0283	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0284	<BatchCount type="Integer" value="1"/>
0285	</ResponseHeader>
0286	<BatchItem>
0287	<Operation type="Enumeration" value="Revoke"/>
0288	<ResultStatus type="Enumeration" value="Success"/>
0289	<ResponsePayload>
0290	<UniqueIdentifier type="TextString"
0291	value="\$UNIQUE_IDENTIFIER_0"/>
0292	</ResponsePayload>
0293	</BatchItem>
0294	</ResponseMessage>
0295	# TIME 6
0296	<RequestMessage>
0297	<RequestHeader>
0298	<ProtocolVersion>
0299	<ProtocolVersionMajor type="Integer" value="1"/>
0300	<ProtocolVersionMinor type="Integer" value="2"/>
0301	</ProtocolVersion>
0302	<BatchCount type="Integer" value="1"/>
0303	</RequestHeader>
0304	<BatchItem>
0305	<Operation type="Enumeration" value="Destroy"/>
0306	<RequestPayload>
0307	<UniqueIdentifier type="TextString"
0308	value="\$UNIQUE_IDENTIFIER_0"/>
0309	</RequestPayload>
0310	</BatchItem>
0311	</RequestMessage>
0312	<ResponseMessage>
0313	<ResponseHeader>
0314	<ProtocolVersion>
0315	<ProtocolVersionMajor type="Integer" value="1"/>
0316	<ProtocolVersionMinor type="Integer" value="2"/>
0317	</ProtocolVersion>
0318	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
	<BatchCount type="Integer" value="1"/>
	</ResponseHeader>
	<BatchItem>
	<Operation type="Enumeration" value="Destroy"/>
	<ResultStatus type="Enumeration" value="Success"/>

0319	<ResponsePayload>
0320	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0321	</ResponsePayload>
0322	</BatchItem>
0323	</ResponseMessage>

960

961 2.3.29 TC-142-12 - Key Wrapping using AES Key Wrap with Attributes

962 Register a 128-bit AES key encryption key (KEK) with the Cryptographic Usage Mask attribute set
963 to Wrap and the Cryptographic Parameters specifying NIST Key Wrap as the Block Cipher Mode.
964 Subsequently, register another 128-bit AES data key (DEK). Retrieve the DEK wrapped using the
965 NIST Key Wrap algorithm and the KEK. The Cryptographic Usage Mask Attribute Name is
966 specified, indicating to the server that this attribute is to be wrapped together with the key
967 material. The Encoding Option field is omitted, which means that the default TTLV-encoding is
968 used. Finally, destroy both keys to return the server to the initial state.

969 The key material for both the KEK and the DEK are from the test vectors specified in Section 4.6
970 of [NISTKeyWrap].

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Name"/>
0016	<AttributeValue>
0017	<NameValue type="TextString" value="TC-142-12-key1"/>
0018	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0019	</AttributeValue>
0020	</Attribute>
0021	<Attribute>
0022	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0023	<AttributeValue type="Integer" value="WrapKey"/>
0024	</Attribute>
0025	<Attribute>
0026	<AttributeName type="TextString" value="Cryptographic
	Parameters"/>
0027	<AttributeValue>
0028	<BlockCipherMode type="Enumeration"
	value="NISTKeyWrap"/>

0029	</AttributeValue>
0030	</Attribute>
0031	<Attribute>
0032	<AttributeName type="TextString" value="Activation Date"/>
0033	<AttributeValue type="DateTime" value="\$NOW-3600"/>
0034	</Attribute>
0035	</TemplateAttribute>
0036	<SymmetricKey>
0037	<KeyBlock>
0038	<KeyFormatType type="Enumeration" value="Raw"/>
0039	<KeyValue>
0040	<KeyMaterial type="ByteString"
	value="000102030405060708090a0b0c0d0e0f"/>
0041	</KeyValue>
0042	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0043	<CryptographicLength type="Integer" value="128"/>
0044	</KeyBlock>
0045	</SymmetricKey>
0046	</RequestPayload>
0047	</BatchItem>
0048	</RequestMessage>
0049	<ResponseMessage>
0050	<ResponseHeader>
0051	<ProtocolVersion>
0052	<ProtocolVersionMajor type="Integer" value="1"/>
0053	<ProtocolVersionMinor type="Integer" value="2"/>
0054	</ProtocolVersion>
0055	<TimeStamp type="DateTime" value="2012-04-27T08:14:42+00:00"/>
0056	<BatchCount type="Integer" value="1"/>
0057	</ResponseHeader>
0058	<BatchItem>
0059	<Operation type="Enumeration" value="Register"/>
0060	<ResultStatus type="Enumeration" value="Success"/>
0061	<ResponsePayload>
0062	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0063	</ResponsePayload>
0064	</BatchItem>
0065	</ResponseMessage>
	# TIME 1
0066	<RequestMessage>
0067	<RequestHeader>
0068	<ProtocolVersion>
0069	<ProtocolVersionMajor type="Integer" value="1"/>
0070	<ProtocolVersionMinor type="Integer" value="2"/>
0071	</ProtocolVersion>
0072	<BatchCount type="Integer" value="1"/>
0073	</RequestHeader>
0074	<BatchItem>
0075	<Operation type="Enumeration" value="Register"/>
0076	<RequestPayload>
0077	<ObjectType type="Enumeration" value="SymmetricKey"/>
0078	<TemplateAttribute>
0079	<Attribute>
0080	<AttributeName type="TextString" value="Name"/>
0081	<AttributeValue>
0082	<NameValue type="TextString" value="TC-142-12-key2"/>

0083	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0084	</AttributeValue>
0085	</Attribute>
0086	<Attribute>
0087	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0088	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0089	</Attribute>
0090	</TemplateAttribute>
0091	<SymmetricKey>
0092	<KeyBlock>
0093	<KeyFormatType type="Enumeration" value="Raw"/>
0094	<KeyValue>
0095	<KeyMaterial type="ByteString"
	value="00112233445566778899aabbccddeeff"/>
0096	</KeyValue>
0097	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0098	<CryptographicLength type="Integer" value="128"/>
0099	</KeyBlock>
0100	</SymmetricKey>
0101	</RequestPayload>
0102	</BatchItem>
0103	</RequestMessage>
0104	<ResponseMessage>
0105	<ResponseHeader>
0106	<ProtocolVersion>
0107	<ProtocolVersionMajor type="Integer" value="1"/>
0108	<ProtocolVersionMinor type="Integer" value="2"/>
0109	</ProtocolVersion>
0110	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0111	<BatchCount type="Integer" value="1"/>
0112	</ResponseHeader>
0113	<BatchItem>
0114	<Operation type="Enumeration" value="Register"/>
0115	<ResultStatus type="Enumeration" value="Success"/>
0116	<ResponsePayload>
0117	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0118	</ResponsePayload>
0119	</BatchItem>
0120	</ResponseMessage>
	# TIME 2
0121	<RequestMessage>
0122	<RequestHeader>
0123	<ProtocolVersion>
0124	<ProtocolVersionMajor type="Integer" value="1"/>
0125	<ProtocolVersionMinor type="Integer" value="2"/>
0126	</ProtocolVersion>
0127	<BatchCount type="Integer" value="1"/>
0128	</RequestHeader>
0129	<BatchItem>
0130	<Operation type="Enumeration" value="Get"/>
0131	<RequestPayload>
0132	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0133	<KeyWrappingSpecification>

0134	<WrappingMethod type="Enumeration" value="Encrypt"/>
0135	<EncryptionKeyInformation>
0136	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0137	<CryptographicParameters>
0138	<BlockCipherMode type="Enumeration"
	value="NISTKeyWrap"/>
0139	</CryptographicParameters>
0140	</EncryptionKeyInformation>
0141	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0142	</KeyWrappingSpecification>
0143	</RequestPayload>
0144	</BatchItem>
0145	</RequestMessage>
0146	<ResponseMessage>
0147	<ResponseHeader>
0148	<ProtocolVersion>
0149	<ProtocolVersionMajor type="Integer" value="1"/>
0150	<ProtocolVersionMinor type="Integer" value="2"/>
0151	</ProtocolVersion>
0152	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0153	<BatchCount type="Integer" value="1"/>
0154	</ResponseHeader>
0155	<BatchItem>
0156	<Operation type="Enumeration" value="Get"/>
0157	<ResultStatus type="Enumeration" value="Success"/>
0158	<ResponsePayload>
0159	<ObjectType type="Enumeration" value="SymmetricKey"/>
0160	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0161	<SymmetricKey>
0162	<KeyBlock>
0163	<KeyFormatType type="Enumeration" value="Raw"/>
0164	<KeyValue type="ByteString"
	value="0dc0f8cb416e7b4422d85805d3dd80e49c6c75f763d1be99748de568e4eec dc05b94b1c1946fd3def14cfe184daada0daf07c93e038ceb9f501bdd8a82c7d6b33 152dbf9d415924b9f13f6cb75ff880ab09dc862e473f74bdaf9398ec7695d41"/>
0165	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0166	<CryptographicLength type="Integer" value="128"/>
0167	<KeyWrappingData>
0168	<WrappingMethod type="Enumeration" value="Encrypt"/>
0169	<EncryptionKeyInformation>
0170	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0171	<CryptographicParameters>
0172	<BlockCipherMode type="Enumeration"
	value="NISTKeyWrap"/>
0173	</CryptographicParameters>
0174	</EncryptionKeyInformation>
0175	</KeyWrappingData>
0176	</KeyBlock>
0177	</SymmetricKey>
0178	</ResponsePayload>
0179	</BatchItem>
0180	</ResponseMessage>
	# TIME 3

0181	<RequestMessage>
0182	<RequestHeader>
0183	<ProtocolVersion>
0184	<ProtocolVersionMajor type="Integer" value="1"/>
0185	<ProtocolVersionMinor type="Integer" value="2"/>
0186	</ProtocolVersion>
0187	<BatchCount type="Integer" value="1"/>
0188	</RequestHeader>
0189	<BatchItem>
0190	<Operation type="Enumeration" value="Get"/>
0191	<RequestPayload>
0192	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0193	</RequestPayload>
0194	</BatchItem>
0195	</RequestMessage>
0196	<ResponseMessage>
0197	<ResponseHeader>
0198	<ProtocolVersion>
0199	<ProtocolVersionMajor type="Integer" value="1"/>
0200	<ProtocolVersionMinor type="Integer" value="2"/>
0201	</ProtocolVersion>
0202	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0203	<BatchCount type="Integer" value="1"/>
0204	</ResponseHeader>
0205	<BatchItem>
0206	<Operation type="Enumeration" value="Get"/>
0207	<ResultStatus type="Enumeration" value="Success"/>
0208	<ResponsePayload>
0209	<ObjectType type="Enumeration" value="SymmetricKey"/>
0210	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0211	<SymmetricKey>
0212	<KeyBlock>
0213	<KeyFormatType type="Enumeration" value="Raw"/>
0214	<KeyValue>
0215	<KeyMaterial type="ByteString"
	value="00112233445566778899aabbccddeeff"/>
0216	</KeyValue>
0217	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0218	<CryptographicLength type="Integer" value="128"/>
0219	</KeyBlock>
0220	</SymmetricKey>
0221	</ResponsePayload>
0222	</BatchItem>
0223	</ResponseMessage>
	# TIME 4
0224	<RequestMessage>
0225	<RequestHeader>
0226	<ProtocolVersion>
0227	<ProtocolVersionMajor type="Integer" value="1"/>
0228	<ProtocolVersionMinor type="Integer" value="2"/>
0229	</ProtocolVersion>
0230	<BatchCount type="Integer" value="1"/>
0231	</RequestHeader>
0232	<BatchItem>
0233	<Operation type="Enumeration" value="Destroy"/>

0234	<RequestPayload>
0235	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0236	</RequestPayload>
0237	</BatchItem>
0238	</RequestMessage>
0239	<ResponseMessage>
0240	<ResponseHeader>
0241	<ProtocolVersion>
0242	<ProtocolVersionMajor type="Integer" value="1"/>
0243	<ProtocolVersionMinor type="Integer" value="2"/>
0244	</ProtocolVersion>
0245	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0246	<BatchCount type="Integer" value="1"/>
0247	</ResponseHeader>
0248	<BatchItem>
0249	<Operation type="Enumeration" value="Destroy"/>
0250	<ResultStatus type="Enumeration" value="Success"/>
0251	<ResponsePayload>
0252	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0253	</ResponsePayload>
0254	</BatchItem>
0255	</ResponseMessage>
	# TIME 5
0256	<RequestMessage>
0257	<RequestHeader>
0258	<ProtocolVersion>
0259	<ProtocolVersionMajor type="Integer" value="1"/>
0260	<ProtocolVersionMinor type="Integer" value="2"/>
0261	</ProtocolVersion>
0262	<BatchCount type="Integer" value="1"/>
0263	</RequestHeader>
0264	<BatchItem>
0265	<Operation type="Enumeration" value="Revoke"/>
0266	<RequestPayload>
0267	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0268	<RevocationReason>
0269	<RevocationReasonCode type="Enumeration"
	value="Unspecified"/>
0270	</RevocationReason>
0271	</RequestPayload>
0272	</BatchItem>
0273	</RequestMessage>
0274	<ResponseMessage>
0275	<ResponseHeader>
0276	<ProtocolVersion>
0277	<ProtocolVersionMajor type="Integer" value="1"/>
0278	<ProtocolVersionMinor type="Integer" value="2"/>
0279	</ProtocolVersion>
0280	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0281	<BatchCount type="Integer" value="1"/>
0282	</ResponseHeader>
0283	<BatchItem>
0284	<Operation type="Enumeration" value="Revoke"/>

0285	<ResultStatus type="Enumeration" value="Success"/>
0286	<ResponsePayload>
0287	<UniqueIdentifier type="TextString"
0288	value="\$UNIQUE_IDENTIFIER_0"/>
0289	</ResponsePayload>
0290	</BatchItem>
0291	</ResponseMessage>
# TIME 6	
0291	<RequestMessage>
0292	<RequestHeader>
0293	<ProtocolVersion>
0294	<ProtocolVersionMajor type="Integer" value="1"/>
0295	<ProtocolVersionMinor type="Integer" value="2"/>
0296	</ProtocolVersion>
0297	<BatchCount type="Integer" value="1"/>
0298	</RequestHeader>
0299	<BatchItem>
0300	<Operation type="Enumeration" value="Destroy"/>
0301	<RequestPayload>
0302	<UniqueIdentifier type="TextString"
0303	value="\$UNIQUE_IDENTIFIER_0"/>
0304	</RequestPayload>
0305	</BatchItem>
0306	</RequestMessage>
0306	<ResponseMessage>
0307	<ResponseHeader>
0308	<ProtocolVersion>
0309	<ProtocolVersionMajor type="Integer" value="1"/>
0310	<ProtocolVersionMinor type="Integer" value="2"/>
0311	</ProtocolVersion>
0312	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0313	<BatchCount type="Integer" value="1"/>
0314	</ResponseHeader>
0315	<BatchItem>
0316	<Operation type="Enumeration" value="Destroy"/>
0317	<ResultStatus type="Enumeration" value="Success"/>
0318	<ResponsePayload>
0319	<UniqueIdentifier type="TextString"
0320	value="\$UNIQUE_IDENTIFIER_0"/>
0321	</ResponsePayload>
0322	</BatchItem>
0322	</ResponseMessage>

971

972 2.3.30 TC-151-12 - Locate a Fresh Object from the Default Group

973 Locate a single fresh object from the default object group. Perform a Get Attribute to retrieve
974 the value of the Fresh attribute to make sure that the key is fresh. Get the object (the kind of
975 object returned depends on the server policy), and get the Fresh attribute again to verify that
976 the object is no longer fresh. Finally, destroy the object. This test case illustrates only one
977 possible behavior related to the default group. In this test case, it is assumed that the server has
978 fresh objects available in the default group, or that it creates a new object on-the-fly as a
979 consequence of the Locate request. It is also assumed that no other client retrieves the object

980 after the Locate but before the batched Get Attributes request, thereby toggling the value of the
981 Fresh attribute.

	<i># TIME 0</i>
0001	<RequestMessage> <RequestHeader>
0002	<ProtocolVersion>
0003	<ProtocolVersionMajor type="Integer" value="1"/>
0004	<ProtocolVersionMinor type="Integer" value="2"/>
0005	</ProtocolVersion>
0006	<BatchOrderOption type="Boolean" value="true"/>
0007	<BatchCount type="Integer" value="2"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Locate"/>
0011	<UniqueBatchItemID type="ByteString" value="1e766d8a95d6e5d1"/>
0012	<RequestPayload>
0013	<MaximumItems type="Integer" value="1"/>
0014	<ObjectGroupMember type="Enumeration"
	value="GroupMemberFresh"/>
0015	<Attribute>
0016	<AttributeName type="TextString" value="Object Group"/>
0017	<AttributeValue type="TextString" value="default"/>
0018	</Attribute>
0019	</RequestPayload>
0020	</BatchItem>
0021	<BatchItem>
0022	<Operation type="Enumeration" value="GetAttributes"/>
0023	<UniqueBatchItemID type="ByteString" value="8650f83be5373722"/>
0024	<RequestPayload>
0025	<AttributeName type="TextString" value="Fresh"/>
0026	</RequestPayload>
0027	</BatchItem>
0028	</RequestMessage>
0029	<ResponseMessage>
0030	<ResponseHeader>
0031	<ProtocolVersion>
0032	<ProtocolVersionMajor type="Integer" value="1"/>
0033	<ProtocolVersionMinor type="Integer" value="2"/>
0034	</ProtocolVersion>
0035	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0036	<BatchCount type="Integer" value="2"/>
0037	</ResponseHeader>
0038	<BatchItem>
0039	<Operation type="Enumeration" value="Locate"/>
0040	<UniqueBatchItemID type="ByteString" value="1e766d8a95d6e5d1"/>
0041	<ResultStatus type="Enumeration" value="Success"/>
0042	<ResponsePayload>
0043	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0044	</ResponsePayload>
0045	</BatchItem>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="GetAttributes"/>
0048	<UniqueBatchItemID type="ByteString" value="8650f83be5373722"/>
0049	<ResultStatus type="Enumeration" value="Success"/>
0050	<ResponsePayload>

0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	<Attribute>
0053	<AttributeName type="TextString" value="Fresh"/>
0054	<AttributeValue type="Boolean" value="true"/>
0055	</Attribute>
0056	</ResponsePayload>
0057	</BatchItem>
0058	</ResponseMessage>
# TIME 1	
0059	<RequestMessage>
0060	<RequestHeader>
0061	<ProtocolVersion>
0062	<ProtocolVersionMajor type="Integer" value="1"/>
0063	<ProtocolVersionMinor type="Integer" value="2"/>
0064	</ProtocolVersion>
0065	<BatchCount type="Integer" value="1"/>
0066	</RequestHeader>
0067	<BatchItem>
0068	<Operation type="Enumeration" value="Get"/>
0069	<RequestPayload>
0070	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0071	</RequestPayload>
0072	</BatchItem>
0073	</RequestMessage>
0074	<ResponseMessage>
0075	<ResponseHeader>
0076	<ProtocolVersion>
0077	<ProtocolVersionMajor type="Integer" value="1"/>
0078	<ProtocolVersionMinor type="Integer" value="2"/>
0079	</ProtocolVersion>
0080	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0081	<BatchCount type="Integer" value="1"/>
0082	</ResponseHeader>
0083	<BatchItem>
0084	<Operation type="Enumeration" value="Get"/>
0085	<ResultStatus type="Enumeration" value="Success"/>
0086	<ResponsePayload>
0087	<ObjectType type="Enumeration" value="SymmetricKey"/>
0088	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0089	<SymmetricKey>
0090	<KeyBlock>
0091	<KeyFormatType type="Enumeration" value="Raw"/>
0092	<KeyValue>
0093	<KeyMaterial type="ByteString"
	value="7fe09d434868ae14a0021ac19330f8d9226790d680e519f8ac25f42d72f60f0c"/>
0094	</KeyValue>
0095	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0096	<CryptographicLength type="Integer" value="256"/>
0097	</KeyBlock>
0098	</SymmetricKey>
0099	</ResponsePayload>
0100	</BatchItem>
0101	</ResponseMessage>

0102	# TIME 2
0103	<RequestMessage>
0104	<RequestHeader>
0105	<ProtocolVersion>
0106	<ProtocolVersionMajor type="Integer" value="1"/>
0107	<ProtocolVersionMinor type="Integer" value="2"/>
0108	</ProtocolVersion>
0109	<BatchCount type="Integer" value="1"/>
0110	</RequestHeader>
0111	<BatchItem>
0112	<Operation type="Enumeration" value="GetAttributes"/>
0113	<RequestPayload>
0114	<UniqueIdentifier type="TextString"
0115	value="\$UNIQUE_IDENTIFIER_0"/>
0116	<AttributeName type="TextString" value="Fresh"/>
0117	</RequestPayload>
0118	</BatchItem>
0119	</RequestMessage>
0120	<ResponseMessage>
0121	<ResponseHeader>
0122	<ProtocolVersion>
0123	<ProtocolVersionMajor type="Integer" value="1"/>
0124	<ProtocolVersionMinor type="Integer" value="2"/>
0125	</ProtocolVersion>
0126	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0127	<BatchCount type="Integer" value="1"/>
0128	</ResponseHeader>
0129	<BatchItem>
0130	<Operation type="Enumeration" value="GetAttributes"/>
0131	<ResultStatus type="Enumeration" value="Success"/>
0132	<ResponsePayload>
0133	<UniqueIdentifier type="TextString"
0134	value="\$UNIQUE_IDENTIFIER_0"/>
0135	<Attribute>
0136	<AttributeName type="TextString" value="Fresh"/>
0137	<AttributeValue type="Boolean" value="false"/>
0138	</Attribute>
0139	</ResponsePayload>
0140	</BatchItem>
0141	</ResponseMessage>
0142	# TIME 3
0143	<RequestMessage>
0144	<RequestHeader>
0145	<ProtocolVersion>
0146	<ProtocolVersionMajor type="Integer" value="1"/>
0147	<ProtocolVersionMinor type="Integer" value="2"/>
0148	</ProtocolVersion>
0149	<BatchCount type="Integer" value="1"/>
0150	</RequestHeader>
0151	<BatchItem>
0152	<Operation type="Enumeration" value="Destroy"/>
0153	<RequestPayload>
0154	<UniqueIdentifier type="TextString"
0155	value="\$UNIQUE_IDENTIFIER_0"/>
0156	</RequestPayload>
0157	</BatchItem>
0158	</RequestMessage>

```
0154 <ResponseMessage>
0155   <ResponseHeader>
0156     <ProtocolVersion>
0157       <ProtocolVersionMajor type="Integer" value="1"/>
0158       <ProtocolVersionMinor type="Integer" value="2"/>
0159     </ProtocolVersion>
0160     <TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0161     <BatchCount type="Integer" value="1"/>
0162   </ResponseHeader>
0163   <BatchItem>
0164     <Operation type="Enumeration" value="Destroy"/>
0165     <ResultStatus type="Enumeration" value="Success"/>
0166     <ResponsePayload>
0167       <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0168     </ResponsePayload>
0169   </BatchItem>
0170 </ResponseMessage>
```

982

983 2.3.31 TC-152-12 - Client-side Group Management

984 Register two symmetric keys, both with the same (non-default) Object Group name specified
985 and the Fresh attribute set to true. Get the Fresh attribute from both keys to make sure it was
986 set. Perform three batched Locate and Get requests to get a fresh key from the group. The first
987 two requests should return both the registered keys, whereas the third request should return no
988 key. To clean up, destroy both keys. This test case assumes that the server supports and sets
989 the Fresh attribute when requested to do so by the client.

```
# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="2"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="Register"/>
0011     <RequestPayload>
0012       <ObjectType type="Enumeration" value="SymmetricKey"/>
0013       <TemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0016           <AttributeValue type="Enumeration" value="AES"/>
0017         </Attribute>
0018         <Attribute>
0019           <AttributeName type="TextString" value="Cryptographic
Length"/>
0020           <AttributeValue type="Integer" value="256"/>
0021         </Attribute>
0022         <Attribute>
0023           <AttributeName type="TextString" value="Cryptographic
```

0024	Usage Mask"/>
0025	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0026	</Attribute>
0027	<Attribute>
0028	<AttributeName type="TextString" value="Object Group"/>
0029	<AttributeValue type="TextString"
0030	value="ClientFreshTest"/>
0031	</Attribute>
0032	<Attribute>
0033	<AttributeName type="TextString" value="Fresh"/>
0034	<AttributeValue type="Boolean" value="true"/>
0035	</Attribute>
0036	<Attribute>
0037	<AttributeName type="TextString" value="x-ID"/>
0038	<AttributeValue type="TextString" value="TC-152-12-key1"/>
0039	</Attribute>
0040	</TemplateAttribute>
0041	<SymmetricKey>
0042	<KeyBlock>
0043	<KeyFormatType type="Enumeration" value="Raw"/>
0044	<KeyValue>
0045	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0046	<CryptographicLength type="Integer" value="256"/>
0047	</KeyBlock>
0048	</SymmetricKey>
0049	</RequestPayload>
0050	</BatchItem>
0051	</RequestMessage>
0052	<ResponseMessage>
0053	<ResponseHeader>
0054	<ProtocolVersion>
0055	<ProtocolVersionMajor type="Integer" value="1"/>
0056	<ProtocolVersionMinor type="Integer" value="2"/>
0057	</ProtocolVersion>
0058	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0059	<BatchCount type="Integer" value="1"/>
0060	</ResponseHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<ResultStatus type="Enumeration" value="Success"/>
0064	<ResponsePayload>
0065	<UniqueIdentifier type="TextString"
0066	value="\$UNIQUE_IDENTIFIER_0"/>
0067	</ResponsePayload>
0068	</BatchItem>
0069	</ResponseMessage>
0070	# TIME 1
0071	<RequestMessage>
0072	<RequestHeader>
0073	<ProtocolVersion>
0074	<ProtocolVersionMajor type="Integer" value="1"/>
	<ProtocolVersionMinor type="Integer" value="2"/>
	</ProtocolVersion>

0075	<BatchCount type="Integer" value="1"/>
0076	</RequestHeader>
0077	<BatchItem>
0078	<Operation type="Enumeration" value="Register"/>
0079	<RequestPayload>
0080	<ObjectType type="Enumeration" value="SymmetricKey"/>
0081	<TemplateAttribute>
0082	<Attribute>
0083	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0084	<AttributeValue type="Enumeration" value="AES"/>
0085	</Attribute>
0086	<Attribute>
0087	<AttributeName type="TextString" value="Cryptographic Length"/>
0088	<AttributeValue type="Integer" value="256"/>
0089	</Attribute>
0090	<Attribute>
0091	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0092	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0093	</Attribute>
0094	<Attribute>
0095	<AttributeName type="TextString" value="Object Group"/>
0096	<AttributeValue type="TextString" value="ClientFreshTest"/>
0097	</Attribute>
0098	<Attribute>
0099	<AttributeName type="TextString" value="Fresh"/>
0100	<AttributeValue type="Boolean" value="true"/>
0101	</Attribute>
0102	<Attribute>
0103	<AttributeName type="TextString" value="x-ID"/>
0104	<AttributeValue type="TextString" value="TC-152-12-key2"/>
0105	</Attribute>
0106	</TemplateAttribute>
0107	<SymmetricKey>
0108	<KeyBlock>
0109	<KeyFormatType type="Enumeration" value="Raw"/>
0110	<KeyValue>
0111	<KeyMaterial type="ByteString" value="00112233445566778899aabbccddeeff000102030405060708090a0b0c0d0 e0f"/>
0112	</KeyValue>
0113	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0114	<CryptographicLength type="Integer" value="256"/>
0115	</KeyBlock>
0116	</SymmetricKey>
0117	</RequestPayload>
0118	</BatchItem>
0119	</RequestMessage>
0120	<ResponseMessage>
0121	<ResponseHeader>
0122	<ProtocolVersion>
0123	<ProtocolVersionMajor type="Integer" value="1"/>
0124	<ProtocolVersionMinor type="Integer" value="2"/>
0125	</ProtocolVersion>

0126	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0127	<BatchCount type="Integer" value="1"/>
0128	</ResponseHeader>
0129	<BatchItem>
0130	<Operation type="Enumeration" value="Register"/>
0131	<ResultStatus type="Enumeration" value="Success"/>
0132	<ResponsePayload>
0133	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0134	</ResponsePayload>
0135	</BatchItem>
0136	</ResponseMessage>
	# TIME 2
0137	<RequestMessage>
0138	<RequestHeader>
0139	<ProtocolVersion>
0140	<ProtocolVersionMajor type="Integer" value="1"/>
0141	<ProtocolVersionMinor type="Integer" value="2"/>
0142	</ProtocolVersion>
0143	<BatchCount type="Integer" value="1"/>
0144	</RequestHeader>
0145	<BatchItem>
0146	<Operation type="Enumeration" value="GetAttributes"/>
0147	<RequestPayload>
0148	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0149	<AttributeName type="TextString" value="Fresh"/>
0150	</RequestPayload>
0151	</BatchItem>
0152	</RequestMessage>
0153	<ResponseMessage>
0154	<ResponseHeader>
0155	<ProtocolVersion>
0156	<ProtocolVersionMajor type="Integer" value="1"/>
0157	<ProtocolVersionMinor type="Integer" value="2"/>
0158	</ProtocolVersion>
0159	<TimeStamp type="DateTime" value="2012-04-27T08:14:43+00:00"/>
0160	<BatchCount type="Integer" value="1"/>
0161	</ResponseHeader>
0162	<BatchItem>
0163	<Operation type="Enumeration" value="GetAttributes"/>
0164	<ResultStatus type="Enumeration" value="Success"/>
0165	<ResponsePayload>
0166	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0167	<Attribute>
0168	<AttributeName type="TextString" value="Fresh"/>
0169	<AttributeValue type="Boolean" value="true"/>
0170	</Attribute>
0171	</ResponsePayload>
0172	</BatchItem>
0173	</ResponseMessage>
	# TIME 3
0174	<RequestMessage>
0175	<RequestHeader>
0176	<ProtocolVersion>

0177	<ProtocolVersionMajor type="Integer" value="1"/>
0178	<ProtocolVersionMinor type="Integer" value="2"/>
0179	</ProtocolVersion>
0180	<BatchCount type="Integer" value="1"/>
0181	</RequestHeader>
0182	<BatchItem>
0183	<Operation type="Enumeration" value="GetAttributes"/>
0184	<RequestPayload>
0185	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0186	<AttributeName type="TextString" value="Fresh"/>
0187	</RequestPayload>
0188	</BatchItem>
0189	</RequestMessage>
0190	<ResponseMessage>
0191	<ResponseHeader>
0192	<ProtocolVersion>
0193	<ProtocolVersionMajor type="Integer" value="1"/>
0194	<ProtocolVersionMinor type="Integer" value="2"/>
0195	</ProtocolVersion>
0196	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0197	<BatchCount type="Integer" value="1"/>
0198	</ResponseHeader>
0199	<BatchItem>
0200	<Operation type="Enumeration" value="GetAttributes"/>
0201	<ResultStatus type="Enumeration" value="Success"/>
0202	<ResponsePayload>
0203	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0204	<Attribute>
0205	<AttributeName type="TextString" value="Fresh"/>
0206	<AttributeValue type="Boolean" value="true"/>
0207	</Attribute>
0208	</ResponsePayload>
0209	</BatchItem>
0210	</ResponseMessage>
	# TIME 4
0211	<RequestMessage>
0212	<RequestHeader>
0213	<ProtocolVersion>
0214	<ProtocolVersionMajor type="Integer" value="1"/>
0215	<ProtocolVersionMinor type="Integer" value="2"/>
0216	</ProtocolVersion>
0217	<BatchOrderOption type="Boolean" value="true"/>
0218	<BatchCount type="Integer" value="2"/>
0219	</RequestHeader>
0220	<BatchItem>
0221	<Operation type="Enumeration" value="Locate"/>
0222	<UniqueBatchItemID type="ByteString" value="294fb5e3e93f8ecc"/>
0223	<RequestPayload>
0224	<MaximumItems type="Integer" value="1"/>
0225	<ObjectGroupMember type="Enumeration"
	value="GroupMemberFresh"/>
0226	<Attribute>
0227	<AttributeName type="TextString" value="Object Group"/>
0228	<AttributeValue type="TextString" value="ClientFreshTest"/>
0229	</Attribute>

0230	</RequestPayload>
0231	</BatchItem>
0232	<BatchItem>
0233	<Operation type="Enumeration" value="Get"/>
0234	<UniqueBatchItemID type="ByteString" value="9da79a935d4e4ae6"/>
0235	<RequestPayload>
0236	</RequestPayload>
0237	</BatchItem>
0238	</RequestMessage>
0239	<ResponseMessage>
0240	<ResponseHeader>
0241	<ProtocolVersion>
0242	<ProtocolVersionMajor type="Integer" value="1"/>
0243	<ProtocolVersionMinor type="Integer" value="2"/>
0244	</ProtocolVersion>
0245	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0246	<BatchCount type="Integer" value="2"/>
0247	</ResponseHeader>
0248	<BatchItem>
0249	<Operation type="Enumeration" value="Locate"/>
0250	<UniqueBatchItemID type="ByteString" value="294fb5e3e93f8ecc"/>
0251	<ResultStatus type="Enumeration" value="Success"/>
0252	<ResponsePayload>
0253	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0254	</ResponsePayload>
0255	</BatchItem>
0256	<BatchItem>
0257	<Operation type="Enumeration" value="Get"/>
0258	<UniqueBatchItemID type="ByteString" value="9da79a935d4e4ae6"/>
0259	<ResultStatus type="Enumeration" value="Success"/>
0260	<ResponsePayload>
0261	<ObjectType type="Enumeration" value="SymmetricKey"/>
0262	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0263	<SymmetricKey>
0264	<KeyBlock>
0265	<KeyFormatType type="Enumeration" value="Raw"/>
0266	<KeyValue>
0267	<KeyMaterial type="ByteString" value="000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1 elf"/>
0268	</KeyValue>
0269	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0270	<CryptographicLength type="Integer" value="256"/>
0271	</KeyBlock>
0272	</SymmetricKey>
0273	</ResponsePayload>
0274	</BatchItem>
0275	</ResponseMessage>
# TIME 5	
0276	<RequestMessage>
0277	<RequestHeader>
0278	<ProtocolVersion>
0279	<ProtocolVersionMajor type="Integer" value="1"/>
0280	<ProtocolVersionMinor type="Integer" value="2"/>
0281	</ProtocolVersion>

0282	<BatchOrderOption type="Boolean" value="true"/>
0283	<BatchCount type="Integer" value="2"/>
0284	</RequestHeader>
0285	<BatchItem>
0286	<Operation type="Enumeration" value="Locate"/>
0287	<UniqueBatchItemID type="ByteString" value="85e3e21d14d6df1d"/>
0288	<RequestPayload>
0289	<MaximumItems type="Integer" value="1"/>
0290	<ObjectGroupMember type="Enumeration"
	value="GroupMemberFresh"/>
0291	<Attribute>
0292	<AttributeName type="TextString" value="Object Group"/>
0293	<AttributeValue type="TextString" value="ClientFreshTest"/>
0294	</Attribute>
0295	</RequestPayload>
0296	</BatchItem>
0297	<BatchItem>
0298	<Operation type="Enumeration" value="Get"/>
0299	<UniqueBatchItemID type="ByteString" value="40feae5ec1bda875"/>
0300	<RequestPayload>
0301	</RequestPayload>
0302	</BatchItem>
0303	</RequestMessage>
0304	<ResponseMessage>
0305	<ResponseHeader>
0306	<ProtocolVersion>
0307	<ProtocolVersionMajor type="Integer" value="1"/>
0308	<ProtocolVersionMinor type="Integer" value="2"/>
0309	</ProtocolVersion>
0310	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0311	<BatchCount type="Integer" value="2"/>
0312	</ResponseHeader>
0313	<BatchItem>
0314	<Operation type="Enumeration" value="Locate"/>
0315	<UniqueBatchItemID type="ByteString" value="85e3e21d14d6df1d"/>
0316	<ResultStatus type="Enumeration" value="Success"/>
0317	<ResponsePayload>
0318	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0319	</ResponsePayload>
0320	</BatchItem>
0321	<BatchItem>
0322	<Operation type="Enumeration" value="Get"/>
0323	<UniqueBatchItemID type="ByteString" value="40feae5ec1bda875"/>
0324	<ResultStatus type="Enumeration" value="Success"/>
0325	<ResponsePayload>
0326	<ObjectType type="Enumeration" value="SymmetricKey"/>
0327	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0328	<SymmetricKey>
0329	<KeyBlock>
0330	<KeyFormatType type="Enumeration" value="Raw"/>
0331	<KeyValue>
0332	<KeyMaterial type="ByteString"
	value="00112233445566778899aabbccddeeff000102030405060708090a0b0c0d0e0f"/>
0333	</KeyValue>

0334	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0335	<CryptographicLength type="Integer" value="256"/>
0336	</KeyBlock>
0337	</SymmetricKey>
0338	</ResponsePayload>
0339	</BatchItem>
0340	</ResponseMessage>
# TIME 6	
0341	<RequestMessage>
0342	<RequestHeader>
0343	<ProtocolVersion>
0344	<ProtocolVersionMajor type="Integer" value="1"/>
0345	<ProtocolVersionMinor type="Integer" value="2"/>
0346	</ProtocolVersion>
0347	<BatchOrderOption type="Boolean" value="true"/>
0348	<BatchCount type="Integer" value="2"/>
0349	</RequestHeader>
0350	<BatchItem>
0351	<Operation type="Enumeration" value="Locate"/>
0352	<UniqueBatchItemID type="ByteString" value="657339bdf375bfa2"/>
0353	<RequestPayload>
0354	<MaximumItems type="Integer" value="1"/>
0355	<ObjectGroupMember type="Enumeration"
0356	value="GroupMemberFresh"/>
0357	<Attribute>
0358	<AttributeName type="TextString" value="Object Group"/>
0359	<AttributeValue type="TextString" value="ClientFreshTest"/>
0360	</Attribute>
0361	</RequestPayload>
0362	</BatchItem>
0363	<BatchItem>
0364	<Operation type="Enumeration" value="Get"/>
0365	<UniqueBatchItemID type="ByteString" value="5713c4911444b36e"/>
0366	<RequestPayload>
0367	</RequestPayload>
0368	</BatchItem>
0369	</RequestMessage>
0370	<ResponseMessage>
0371	<ResponseHeader>
0372	<ProtocolVersion>
0373	<ProtocolVersionMajor type="Integer" value="1"/>
0374	<ProtocolVersionMinor type="Integer" value="2"/>
0375	</ProtocolVersion>
0376	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0377	<BatchCount type="Integer" value="2"/>
0378	</ResponseHeader>
0379	<BatchItem>
0380	<Operation type="Enumeration" value="Locate"/>
0381	<UniqueBatchItemID type="ByteString" value="657339bdf375bfa2"/>
0382	<ResultStatus type="Enumeration" value="Success"/>
0383	<ResponsePayload>
0384	</ResponsePayload>
0385	</BatchItem>
0386	<BatchItem>
0387	<Operation type="Enumeration" value="Get"/>
0388	<UniqueBatchItemID type="ByteString" value="5713c4911444b36e"/>
0389	<ResultStatus type="Enumeration" value="OperationFailed"/>

0389	<ResultReason type="Enumeration" value="ItemNotFound"/>
0390	<ResultMessage type="TextString" value="NOT_FOUND"/>
0391	</BatchItem>
0392	</ResponseMessage>
# TIME 7	
0393	<RequestMessage>
0394	<RequestHeader>
0395	<ProtocolVersion>
0396	<ProtocolVersionMajor type="Integer" value="1"/>
0397	<ProtocolVersionMinor type="Integer" value="2"/>
0398	</ProtocolVersion>
0399	<BatchCount type="Integer" value="1"/>
0400	</RequestHeader>
0401	<BatchItem>
0402	<Operation type="Enumeration" value="Destroy"/>
0403	<RequestPayload>
0404	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0405	</RequestPayload>
0406	</BatchItem>
0407	</RequestMessage>
0408	<ResponseMessage>
0409	<ResponseHeader>
0410	<ProtocolVersion>
0411	<ProtocolVersionMajor type="Integer" value="1"/>
0412	<ProtocolVersionMinor type="Integer" value="2"/>
0413	</ProtocolVersion>
0414	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0415	<BatchCount type="Integer" value="1"/>
0416	</ResponseHeader>
0417	<BatchItem>
0418	<Operation type="Enumeration" value="Destroy"/>
0419	<ResultStatus type="Enumeration" value="Success"/>
0420	<ResponsePayload>
0421	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0422	</ResponsePayload>
0423	</BatchItem>
0424	</ResponseMessage>
# TIME 8	
0425	<RequestMessage>
0426	<RequestHeader>
0427	<ProtocolVersion>
0428	<ProtocolVersionMajor type="Integer" value="1"/>
0429	<ProtocolVersionMinor type="Integer" value="2"/>
0430	</ProtocolVersion>
0431	<BatchCount type="Integer" value="1"/>
0432	</RequestHeader>
0433	<BatchItem>
0434	<Operation type="Enumeration" value="Destroy"/>
0435	<RequestPayload>
0436	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0437	</RequestPayload>
0438	</BatchItem>
0439	</RequestMessage>

```
0440 <ResponseMessage>
0441   <ResponseHeader>
0442     <ProtocolVersion>
0443       <ProtocolVersionMajor type="Integer" value="1"/>
0444       <ProtocolVersionMinor type="Integer" value="2"/>
0445     </ProtocolVersion>
0446     <TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0447     <BatchCount type="Integer" value="1"/>
0448   </ResponseHeader>
0449   <BatchItem>
0450     <Operation type="Enumeration" value="Destroy"/>
0451     <ResultStatus type="Enumeration" value="Success"/>
0452     <ResponsePayload>
0453       <UniqueIdentifier type="TextString"
0454       value="$UNIQUE_IDENTIFIER_1"/>
0455     </ResponsePayload>
0456   </BatchItem>
0457 </ResponseMessage>
```

990

991 2.3.32 TC-153-12 - Default Object Group Member

992 This test case exercises the 'default' Object Group Member flag in the Locate request. Three
993 keys are created on the server and put into the same group (the Object Group attribute is set to
994 the same value for all keys). Thereafter, the client performs four batched Locate and Get
995 requests, asking for the default object from the group. This test case assumes that the server
996 policy is such that it serves objects from the group in a round-robin fashion. The pointer to the
997 default object is advanced each time an object is retrieved using a Get request. The first three
998 times Locate and Get is executed, the three keys are returned one after the other. When Locate
999 and Get is executed for the fourth time, the first key is again returned. Finally, all keys are
1000 destroyed.

1001 Note: there is no requirement for a server to implement support for any round-robin based
1002 allocation; this test case illustrates a server which supports such a policy.

```
0001 # TIME 0
0002 <RequestMessage>
0003   <RequestHeader>
0004     <ProtocolVersion>
0005       <ProtocolVersionMajor type="Integer" value="1"/>
0006       <ProtocolVersionMinor type="Integer" value="2"/>
0007     </ProtocolVersion>
0008     <BatchCount type="Integer" value="3"/>
0009   </RequestHeader>
0010   <BatchItem>
0011     <Operation type="Enumeration" value="Create"/>
0012     <UniqueBatchItemID type="ByteString" value="75e8bdb337aec40e"/>
0013     <RequestPayload>
0014       <ObjectType type="Enumeration" value="SymmetricKey"/>
0015       <TemplateAttribute>
0016         <Attribute>
0017           <AttributeName type="TextString" value="Cryptographic
0018           Algorithm"/>
0019           <AttributeValue type="Enumeration" value="AES"/>
```

0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic Length"/>
0021	<AttributeValue type="Integer" value="256"/>
0022	</Attribute>
0023	<Attribute>
0024	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0025	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0026	</Attribute>
0027	<Attribute>
0028	<AttributeName type="TextString" value="Object Group"/>
0029	<AttributeValue type="TextString" value="RoundRobinTestGroup"/>
0030	</Attribute>
0031	<Attribute>
0032	<AttributeName type="TextString" value="x-ID"/>
0033	<AttributeValue type="TextString" value="TC-153-12-key1"/>
0034	</Attribute>
0035	</TemplateAttribute>
0036	</RequestPayload>
0037	</BatchItem>
0038	<BatchItem>
0039	<Operation type="Enumeration" value="Create"/>
0040	<UniqueBatchItemID type="ByteString" value="ac0e6e56e8d99f66"/>
0041	<RequestPayload>
0042	<ObjectType type="Enumeration" value="SymmetricKey"/>
0043	<TemplateAttribute>
0044	<Attribute>
0045	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0046	<AttributeValue type="Enumeration" value="AES"/>
0047	</Attribute>
0048	<Attribute>
0049	<AttributeName type="TextString" value="Cryptographic Length"/>
0050	<AttributeValue type="Integer" value="256"/>
0051	</Attribute>
0052	<Attribute>
0053	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0054	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0055	</Attribute>
0056	<Attribute>
0057	<AttributeName type="TextString" value="Object Group"/>
0058	<AttributeValue type="TextString" value="RoundRobinTestGroup"/>
0059	</Attribute>
0060	<Attribute>
0061	<AttributeName type="TextString" value="x-ID"/>
0062	<AttributeValue type="TextString" value="TC-153-12-key2"/>
0063	</Attribute>
0064	</TemplateAttribute>
0065	</RequestPayload>
0066	</BatchItem>
0067	<BatchItem>

0068	<Operation type="Enumeration" value="Create"/>
0069	<UniqueBatchItemID type="ByteString" value="77e87d356ba09da1"/>
0070	<RequestPayload>
0071	<ObjectType type="Enumeration" value="SymmetricKey"/>
0072	<TemplateAttribute>
0073	<Attribute>
0074	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0075	<AttributeValue type="Enumeration" value="AES"/>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0079	<AttributeValue type="Integer" value="256"/>
0080	</Attribute>
0081	<Attribute>
0082	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0083	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0084	</Attribute>
0085	<Attribute>
0086	<AttributeName type="TextString" value="Object Group"/>
0087	<AttributeValue type="TextString"
	value="RoundRobinTestGroup"/>
0088	</Attribute>
0089	<Attribute>
0090	<AttributeName type="TextString" value="x-ID"/>
0091	<AttributeValue type="TextString" value="TC-153-12-key3"/>
0092	</Attribute>
0093	</TemplateAttribute>
0094	</RequestPayload>
0095	</BatchItem>
0096	</RequestMessage>
0097	<ResponseMessage>
0098	<ResponseHeader>
0099	<ProtocolVersion>
0100	<ProtocolVersionMajor type="Integer" value="1"/>
0101	<ProtocolVersionMinor type="Integer" value="2"/>
0102	</ProtocolVersion>
0103	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0104	<BatchCount type="Integer" value="3"/>
0105	</ResponseHeader>
0106	<BatchItem>
0107	<Operation type="Enumeration" value="Create"/>
0108	<UniqueBatchItemID type="ByteString" value="75e8bdb337aec40e"/>
0109	<ResultStatus type="Enumeration" value="Success"/>
0110	<ResponsePayload>
0111	<ObjectType type="Enumeration" value="SymmetricKey"/>
0112	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0113	</ResponsePayload>
0114	</BatchItem>
0115	<BatchItem>
0116	<Operation type="Enumeration" value="Create"/>
0117	<UniqueBatchItemID type="ByteString" value="ac0e6e56e8d99f66"/>
0118	<ResultStatus type="Enumeration" value="Success"/>
0119	<ResponsePayload>

0120	<ObjectType type="Enumeration" value="SymmetricKey"/>
0121	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0122	</ResponsePayload>
0123	</BatchItem>
0124	<BatchItem>
0125	<Operation type="Enumeration" value="Create"/>
0126	<UniqueBatchItemID type="ByteString" value="77e87d356ba09da1"/>
0127	<ResultStatus type="Enumeration" value="Success"/>
0128	<ResponsePayload>
0129	<ObjectType type="Enumeration" value="SymmetricKey"/>
0130	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0131	</ResponsePayload>
0132	</BatchItem>
0133	</ResponseMessage>
	# TIME 1
0134	<RequestMessage>
0135	<RequestHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="2"/>
0139	</ProtocolVersion>
0140	<BatchOrderOption type="Boolean" value="true"/>
0141	<BatchCount type="Integer" value="2"/>
0142	</RequestHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="Locate"/>
0145	<UniqueBatchItemID type="ByteString" value="99e7a6ea0125bb67"/>
0146	<RequestPayload>
0147	<MaximumItems type="Integer" value="1"/>
0148	<ObjectGroupMember type="Enumeration"
	value="GroupMemberDefault"/>
0149	<Attribute>
0150	<AttributeName type="TextString" value="Object Group"/>
0151	<AttributeValue type="TextString"
	value="RoundRobinTestGroup"/>
0152	</Attribute>
0153	</RequestPayload>
0154	</BatchItem>
0155	<BatchItem>
0156	<Operation type="Enumeration" value="Get"/>
0157	<UniqueBatchItemID type="ByteString" value="0efd9c2e346ee1cb"/>
0158	<RequestPayload>
0159	</RequestPayload>
0160	</BatchItem>
0161	</RequestMessage>
0162	<ResponseMessage>
0163	<ResponseHeader>
0164	<ProtocolVersion>
0165	<ProtocolVersionMajor type="Integer" value="1"/>
0166	<ProtocolVersionMinor type="Integer" value="2"/>
0167	</ProtocolVersion>
0168	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0169	<BatchCount type="Integer" value="2"/>
0170	</ResponseHeader>
0171	<BatchItem>

0172	<Operation type="Enumeration" value="Locate"/>
0173	<UniqueBatchItemID type="ByteString" value="99e7a6ea0125bb67"/>
0174	<ResultStatus type="Enumeration" value="Success"/>
0175	<ResponsePayload>
0176	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0177	</ResponsePayload>
0178	</BatchItem>
0179	<BatchItem>
0180	<Operation type="Enumeration" value="Get"/>
0181	<UniqueBatchItemID type="ByteString" value="0efd9c2e346ee1cb"/>
0182	<ResultStatus type="Enumeration" value="Success"/>
0183	<ResponsePayload>
0184	<ObjectType type="Enumeration" value="SymmetricKey"/>
0185	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0186	<SymmetricKey>
0187	<KeyBlock>
0188	<KeyFormatType type="Enumeration" value="Raw"/>
0189	<KeyValue>
0190	<KeyMaterial type="ByteString"
	value="bd13da8bce07ea6b89c4d110827bf6a8478cf95edca9bbc278ab04f4cbeecff0"/>
0191	</KeyValue>
0192	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0193	<CryptographicLength type="Integer" value="256"/>
0194	</KeyBlock>
0195	</SymmetricKey>
0196	</ResponsePayload>
0197	</BatchItem>
0198	</ResponseMessage>
	# TIME 2
0199	<RequestMessage>
0200	<RequestHeader>
0201	<ProtocolVersion>
0202	<ProtocolVersionMajor type="Integer" value="1"/>
0203	<ProtocolVersionMinor type="Integer" value="2"/>
0204	</ProtocolVersion>
0205	<BatchOrderOption type="Boolean" value="true"/>
0206	<BatchCount type="Integer" value="2"/>
0207	</RequestHeader>
0208	<BatchItem>
0209	<Operation type="Enumeration" value="Locate"/>
0210	<UniqueBatchItemID type="ByteString" value="0303428f37f17b8d"/>
0211	<RequestPayload>
0212	<MaximumItems type="Integer" value="1"/>
0213	<ObjectGroupMember type="Enumeration"
	value="GroupMemberDefault"/>
0214	<Attribute>
0215	<AttributeName type="TextString" value="Object Group"/>
0216	<AttributeValue type="TextString"
	value="RoundRobinTestGroup"/>
0217	</Attribute>
0218	</RequestPayload>
0219	</BatchItem>
0220	<BatchItem>
0221	<Operation type="Enumeration" value="Get"/>

0222	<UniqueBatchItemID type="ByteString" value="dae46b60d9b6459b"/>
0223	<RequestPayload>
0224	</RequestPayload>
0225	</BatchItem>
0226	</RequestMessage>
0227	<ResponseMessage>
0228	<ResponseHeader>
0229	<ProtocolVersion>
0230	<ProtocolVersionMajor type="Integer" value="1"/>
0231	<ProtocolVersionMinor type="Integer" value="2"/>
0232	</ProtocolVersion>
0233	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0234	<BatchCount type="Integer" value="2"/>
0235	</ResponseHeader>
0236	<BatchItem>
0237	<Operation type="Enumeration" value="Locate"/>
0238	<UniqueBatchItemID type="ByteString" value="0303428f37f17b8d"/>
0239	<ResultStatus type="Enumeration" value="Success"/>
0240	<ResponsePayload>
0241	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0242	</ResponsePayload>
0243	</BatchItem>
0244	<BatchItem>
0245	<Operation type="Enumeration" value="Get"/>
0246	<UniqueBatchItemID type="ByteString" value="dae46b60d9b6459b"/>
0247	<ResultStatus type="Enumeration" value="Success"/>
0248	<ResponsePayload>
0249	<ObjectType type="Enumeration" value="SymmetricKey"/>
0250	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0251	<SymmetricKey>
0252	<KeyBlock>
0253	<KeyFormatType type="Enumeration" value="Raw"/>
0254	<KeyValue>
0255	<KeyMaterial type="ByteString"
	value="430bfb0cbc273e15326e3a23965f7704a13af37a642c37026c9a59694c83b7a3"/>
0256	</KeyValue>
0257	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0258	<CryptographicLength type="Integer" value="256"/>
0259	</KeyBlock>
0260	</SymmetricKey>
0261	</ResponsePayload>
0262	</BatchItem>
0263	</ResponseMessage>
	# TIME 3
0264	<RequestMessage>
0265	<RequestHeader>
0266	<ProtocolVersion>
0267	<ProtocolVersionMajor type="Integer" value="1"/>
0268	<ProtocolVersionMinor type="Integer" value="2"/>
0269	</ProtocolVersion>
0270	<BatchOrderOption type="Boolean" value="true"/>
0271	<BatchCount type="Integer" value="2"/>
0272	</RequestHeader>
0273	<BatchItem>

0274	<Operation type="Enumeration" value="Locate"/>
0275	<UniqueBatchItemID type="ByteString" value="863c27d7a0d3da5e"/>
0276	<RequestPayload>
0277	<MaximumItems type="Integer" value="1"/>
0278	<ObjectGroupMember type="Enumeration"
	value="GroupMemberDefault"/>
0279	<Attribute>
0280	<AttributeName type="TextString" value="Object Group"/>
0281	<AttributeValue type="TextString"
	value="RoundRobinTestGroup"/>
0282	</Attribute>
0283	</RequestPayload>
0284	</BatchItem>
0285	<BatchItem>
0286	<Operation type="Enumeration" value="Get"/>
0287	<UniqueBatchItemID type="ByteString" value="c4617b3205e96fb2"/>
0288	<RequestPayload>
0289	</RequestPayload>
0290	</BatchItem>
0291	</RequestMessage>
0292	<ResponseMessage>
0293	<ResponseHeader>
0294	<ProtocolVersion>
0295	<ProtocolVersionMajor type="Integer" value="1"/>
0296	<ProtocolVersionMinor type="Integer" value="2"/>
0297	</ProtocolVersion>
0298	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0299	<BatchCount type="Integer" value="2"/>
0300	</ResponseHeader>
0301	<BatchItem>
0302	<Operation type="Enumeration" value="Locate"/>
0303	<UniqueBatchItemID type="ByteString" value="863c27d7a0d3da5e"/>
0304	<ResultStatus type="Enumeration" value="Success"/>
0305	<ResponsePayload>
0306	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0307	</ResponsePayload>
0308	</BatchItem>
0309	<BatchItem>
0310	<Operation type="Enumeration" value="Get"/>
0311	<UniqueBatchItemID type="ByteString" value="c4617b3205e96fb2"/>
0312	<ResultStatus type="Enumeration" value="Success"/>
0313	<ResponsePayload>
0314	<ObjectType type="Enumeration" value="SymmetricKey"/>
0315	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0316	<SymmetricKey>
0317	<KeyBlock>
0318	<KeyFormatType type="Enumeration" value="Raw"/>
0319	<KeyValue>
0320	<KeyMaterial type="ByteString"
	value="a51b38e400168a25f2f122d7b8543a00daf022e61677a08a33a834f5f52c3097"/>
0321	</KeyValue>
0322	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0323	<CryptographicLength type="Integer" value="256"/>
0324	</KeyBlock>

0325	</SymmetricKey>
0326	</ResponsePayload>
0327	</BatchItem>
0328	</ResponseMessage>
# TIME 4	
0329	<RequestMessage>
0330	<RequestHeader>
0331	<ProtocolVersion>
0332	<ProtocolVersionMajor type="Integer" value="1"/>
0333	<ProtocolVersionMinor type="Integer" value="2"/>
0334	</ProtocolVersion>
0335	<BatchOrderOption type="Boolean" value="true"/>
0336	<BatchCount type="Integer" value="2"/>
0337	</RequestHeader>
0338	<BatchItem>
0339	<Operation type="Enumeration" value="Locate"/>
0340	<UniqueBatchItemID type="ByteString" value="f1ce9893ee5bde19"/>
0341	<RequestPayload>
0342	<MaximumItems type="Integer" value="1"/>
0343	<ObjectGroupMember type="Enumeration"
	value="GroupMemberDefault"/>
0344	<Attribute>
0345	<AttributeName type="TextString" value="Object Group"/>
0346	<AttributeValue type="TextString"
	value="RoundRobinTestGroup"/>
0347	</Attribute>
0348	</RequestPayload>
0349	</BatchItem>
0350	<BatchItem>
0351	<Operation type="Enumeration" value="Get"/>
0352	<UniqueBatchItemID type="ByteString" value="9a18dd11cc6ce394"/>
0353	<RequestPayload>
0354	</RequestPayload>
0355	</BatchItem>
0356	</RequestMessage>
0357	<ResponseMessage>
0358	<ResponseHeader>
0359	<ProtocolVersion>
0360	<ProtocolVersionMajor type="Integer" value="1"/>
0361	<ProtocolVersionMinor type="Integer" value="2"/>
0362	</ProtocolVersion>
0363	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0364	<BatchCount type="Integer" value="2"/>
0365	</ResponseHeader>
0366	<BatchItem>
0367	<Operation type="Enumeration" value="Locate"/>
0368	<UniqueBatchItemID type="ByteString" value="f1ce9893ee5bde19"/>
0369	<ResultStatus type="Enumeration" value="Success"/>
0370	<ResponsePayload>
0371	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0372	</ResponsePayload>
0373	</BatchItem>
0374	<BatchItem>
0375	<Operation type="Enumeration" value="Get"/>
0376	<UniqueBatchItemID type="ByteString" value="9a18dd11cc6ce394"/>
0377	<ResultStatus type="Enumeration" value="Success"/>

0378	<ResponsePayload>
0379	<ObjectType type="Enumeration" value="SymmetricKey"/>
0380	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0381	<SymmetricKey>
0382	<KeyBlock>
0383	<KeyFormatType type="Enumeration" value="Raw"/>
0384	<KeyValue>
0385	<KeyMaterial type="ByteString"
	value="bd13da8bce07ea6b89c4d110827bf6a8478cf95edca9bbc278ab04f4cbeecff0"/>
0386	</KeyValue>
0387	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0388	<CryptographicLength type="Integer" value="256"/>
0389	</KeyBlock>
0390	</SymmetricKey>
0391	</ResponsePayload>
0392	</BatchItem>
0393	</ResponseMessage>
	# TIME 5
0394	<RequestMessage>
0395	<RequestHeader>
0396	<ProtocolVersion>
0397	<ProtocolVersionMajor type="Integer" value="1"/>
0398	<ProtocolVersionMinor type="Integer" value="2"/>
0399	</ProtocolVersion>
0400	<BatchErrorContinuationOption type="Enumeration"
	value="Continue"/>
0401	<BatchOrderOption type="Boolean" value="true"/>
0402	<BatchCount type="Integer" value="3"/>
0403	</RequestHeader>
0404	<BatchItem>
0405	<Operation type="Enumeration" value="Destroy"/>
0406	<UniqueBatchItemID type="ByteString" value="f4cf0a5614786eb7"/>
0407	<RequestPayload>
0408	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0409	</RequestPayload>
0410	</BatchItem>
0411	<BatchItem>
0412	<Operation type="Enumeration" value="Destroy"/>
0413	<UniqueBatchItemID type="ByteString" value="dd55da10ebe91928"/>
0414	<RequestPayload>
0415	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0416	</RequestPayload>
0417	</BatchItem>
0418	<BatchItem>
0419	<Operation type="Enumeration" value="Destroy"/>
0420	<UniqueBatchItemID type="ByteString" value="18334af52fee87fa"/>
0421	<RequestPayload>
0422	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0423	</RequestPayload>
0424	</BatchItem>
0425	</RequestMessage>
0426	<ResponseMessage>

```

0427 <ResponseHeader>
0428   <ProtocolVersion>
0429     <ProtocolVersionMajor type="Integer" value="1"/>
0430     <ProtocolVersionMinor type="Integer" value="2"/>
0431   </ProtocolVersion>
0432   <TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0433   <BatchCount type="Integer" value="3"/>
0434 </ResponseHeader>
0435 <BatchItem>
0436   <Operation type="Enumeration" value="Destroy"/>
0437   <UniqueBatchItemID type="ByteString" value="f4cf0a5614786eb7"/>
0438   <ResultStatus type="Enumeration" value="Success"/>
0439   <ResponsePayload>
0440     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0441   </ResponsePayload>
0442 </BatchItem>
0443 <BatchItem>
0444   <Operation type="Enumeration" value="Destroy"/>
0445   <UniqueBatchItemID type="ByteString" value="dd55da10ebe91928"/>
0446   <ResultStatus type="Enumeration" value="Success"/>
0447   <ResponsePayload>
0448     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0449   </ResponsePayload>
0450 </BatchItem>
0451 <BatchItem>
0452   <Operation type="Enumeration" value="Destroy"/>
0453   <UniqueBatchItemID type="ByteString" value="18334af52fee87fa"/>
0454   <ResultStatus type="Enumeration" value="Success"/>
0455   <ResponsePayload>
0456     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_2"/>
0457   </ResponsePayload>
0458 </BatchItem>
0459 </ResponseMessage>

```

1003

1004 2.3.33 TC-161-12 - Discover Versions

1005 Exercise the Discover Versions operation in different ways in order to find out which versions a
1006 server supports, as well as to get a list of versions supported by both client and server.

1007 This test case shows the expected responses from a KMIP 1.2 server that supports versions 1.2,
1008 1.1 and 1.0, with 1.2 being the preferred version.

```

0001 # TIME 0
0002 <RequestMessage>
0003   <RequestHeader>
0004     <ProtocolVersion>
0005       <ProtocolVersionMajor type="Integer" value="1"/>
0006       <ProtocolVersionMinor type="Integer" value="2"/>
0007     </ProtocolVersion>
0008     <BatchCount type="Integer" value="1"/>
0009   </RequestHeader>
0010   <BatchItem>

```

0010	<Operation type="Enumeration" value="DiscoverVersions"/>
0011	<RequestPayload>
0012	</RequestPayload>
0013	</BatchItem>
0014	</RequestMessage>
0015	<ResponseMessage>
0016	<ResponseHeader>
0017	<ProtocolVersion>
0018	<ProtocolVersionMajor type="Integer" value="1"/>
0019	<ProtocolVersionMinor type="Integer" value="2"/>
0020	</ProtocolVersion>
0021	<TimeStamp type="DateTime" value="2011-12-01T08:46:15+00:00"/>
0022	<BatchCount type="Integer" value="1"/>
0023	</ResponseHeader>
0024	<BatchItem>
0025	<Operation type="Enumeration" value="DiscoverVersions"/>
0026	<ResultStatus type="Enumeration" value="Success"/>
0027	<ResponsePayload>
0028	<ProtocolVersion>
0029	<ProtocolVersionMajor type="Integer" value="1"/>
0030	<ProtocolVersionMinor type="Integer" value="2"/>
0031	</ProtocolVersion>
0032	<ProtocolVersion>
0033	<ProtocolVersionMajor type="Integer" value="1"/>
0034	<ProtocolVersionMinor type="Integer" value="1"/>
0035	</ProtocolVersion>
0036	<ProtocolVersion>
0037	<ProtocolVersionMajor type="Integer" value="1"/>
0038	<ProtocolVersionMinor type="Integer" value="0"/>
0039	</ProtocolVersion>
0040	</ResponsePayload>
0041	</BatchItem>
0042	</ResponseMessage>
# TIME 1	
0043	<RequestMessage>
0044	<RequestHeader>
0045	<ProtocolVersion>
0046	<ProtocolVersionMajor type="Integer" value="1"/>
0047	<ProtocolVersionMinor type="Integer" value="2"/>
0048	</ProtocolVersion>
0049	<BatchCount type="Integer" value="1"/>
0050	</RequestHeader>
0051	<BatchItem>
0052	<Operation type="Enumeration" value="DiscoverVersions"/>
0053	<RequestPayload>
0054	<ProtocolVersion>
0055	<ProtocolVersionMajor type="Integer" value="1"/>
0056	<ProtocolVersionMinor type="Integer" value="0"/>
0057	</ProtocolVersion>
0058	</RequestPayload>
0059	</BatchItem>
0060	</RequestMessage>
0061	<ResponseMessage>
0062	<ResponseHeader>
0063	<ProtocolVersion>
0064	<ProtocolVersionMajor type="Integer" value="1"/>

0065	<ProtocolVersionMinor type="Integer" value="2"/>
0066	</ProtocolVersion>
0067	<TimeStamp type="DateTime" value="2011-06-24T12:52:18+00:00"/>
0068	<BatchCount type="Integer" value="1"/>
0069	</ResponseHeader>
0070	<BatchItem>
0071	<Operation type="Enumeration" value="DiscoverVersions"/>
0072	<ResultStatus type="Enumeration" value="Success"/>
0073	<ResponsePayload>
0074	<ProtocolVersion>
0075	<ProtocolVersionMajor type="Integer" value="1"/>
0076	<ProtocolVersionMinor type="Integer" value="0"/>
0077	</ProtocolVersion>
0078	</ResponsePayload>
0079	</BatchItem>
0080	</ResponseMessage>
# TIME 2	
0081	<RequestMessage>
0082	<RequestHeader>
0083	<ProtocolVersion>
0084	<ProtocolVersionMajor type="Integer" value="1"/>
0085	<ProtocolVersionMinor type="Integer" value="2"/>
0086	</ProtocolVersion>
0087	<BatchCount type="Integer" value="1"/>
0088	</RequestHeader>
0089	<BatchItem>
0090	<Operation type="Enumeration" value="DiscoverVersions"/>
0091	<RequestPayload>
0092	<ProtocolVersion>
0093	<ProtocolVersionMajor type="Integer" value="1"/>
0094	<ProtocolVersionMinor type="Integer" value="1"/>
0095	</ProtocolVersion>
0096	</RequestPayload>
0097	</BatchItem>
0098	</RequestMessage>
0099	<ResponseMessage>
0100	<ResponseHeader>
0101	<ProtocolVersion>
0102	<ProtocolVersionMajor type="Integer" value="1"/>
0103	<ProtocolVersionMinor type="Integer" value="2"/>
0104	</ProtocolVersion>
0105	<TimeStamp type="DateTime" value="2011-12-01T08:46:15+00:00"/>
0106	<BatchCount type="Integer" value="1"/>
0107	</ResponseHeader>
0108	<BatchItem>
0109	<Operation type="Enumeration" value="DiscoverVersions"/>
0110	<ResultStatus type="Enumeration" value="Success"/>
0111	<ResponsePayload>
0112	<ProtocolVersion>
0113	<ProtocolVersionMajor type="Integer" value="1"/>
0114	<ProtocolVersionMinor type="Integer" value="1"/>
0115	</ProtocolVersion>
0116	</ResponsePayload>
0117	</BatchItem>
0118	</ResponseMessage>
# TIME 3	

0119	<RequestMessage>
0120	<RequestHeader>
0121	<ProtocolVersion>
0122	<ProtocolVersionMajor type="Integer" value="1"/>
0123	<ProtocolVersionMinor type="Integer" value="2"/>
0124	</ProtocolVersion>
0125	<BatchCount type="Integer" value="1"/>
0126	</RequestHeader>
0127	<BatchItem>
0128	<Operation type="Enumeration" value="DiscoverVersions"/>
0129	<RequestPayload>
0130	<ProtocolVersion>
0131	<ProtocolVersionMajor type="Integer" value="1"/>
0132	<ProtocolVersionMinor type="Integer" value="2"/>
0133	</ProtocolVersion>
0134	</RequestPayload>
0135	</BatchItem>
0136	</RequestMessage>
0137	<ResponseMessage>
0138	<ResponseHeader>
0139	<ProtocolVersion>
0140	<ProtocolVersionMajor type="Integer" value="1"/>
0141	<ProtocolVersionMinor type="Integer" value="2"/>
0142	</ProtocolVersion>
0143	<TimeStamp type="DateTime" value="2011-12-01T08:46:15+00:00"/>
0144	<BatchCount type="Integer" value="1"/>
0145	</ResponseHeader>
0146	<BatchItem>
0147	<Operation type="Enumeration" value="DiscoverVersions"/>
0148	<ResultStatus type="Enumeration" value="Success"/>
0149	<ResponsePayload>
0150	<ProtocolVersion>
0151	<ProtocolVersionMajor type="Integer" value="1"/>
0152	<ProtocolVersionMinor type="Integer" value="2"/>
0153	</ProtocolVersion>
0154	</ResponsePayload>
0155	</BatchItem>
0156	</ResponseMessage>
# TIME 4	
0157	<RequestMessage>
0158	<RequestHeader>
0159	<ProtocolVersion>
0160	<ProtocolVersionMajor type="Integer" value="1"/>
0161	<ProtocolVersionMinor type="Integer" value="2"/>
0162	</ProtocolVersion>
0163	<BatchCount type="Integer" value="1"/>
0164	</RequestHeader>
0165	<BatchItem>
0166	<Operation type="Enumeration" value="DiscoverVersions"/>
0167	<RequestPayload>
0168	<ProtocolVersion>
0169	<ProtocolVersionMajor type="Integer" value="9"/>
0170	<ProtocolVersionMinor type="Integer" value="31"/>
0171	</ProtocolVersion>
0172	</RequestPayload>
0173	</BatchItem>
0174	</RequestMessage>

```
0175 <ResponseMessage>
0176   <ResponseHeader>
0177     <ProtocolVersion>
0178       <ProtocolVersionMajor type="Integer" value="1"/>
0179       <ProtocolVersionMinor type="Integer" value="2"/>
0180     </ProtocolVersion>
0181     <TimeStamp type="DateTime" value="2011-12-01T08:46:15+00:00"/>
0182     <BatchCount type="Integer" value="1"/>
0183   </ResponseHeader>
0184   <BatchItem>
0185     <Operation type="Enumeration" value="DiscoverVersions"/>
0186     <ResultStatus type="Enumeration" value="Success"/>
0187     <ResponsePayload>
0188     </ResponsePayload>
0189   </BatchItem>
0190 </ResponseMessage>
```

1009

1010 2.3.34 TC-171-12 - Handling of Attributes and Attribute Index Values

1011 This test case illustrates the changes in Attribute and Attribute Index handling introduced in
1012 KMIP-1.1. A symmetric key is created on the server, and two Name attributes and the Contact
1013 Information attribute is specified for the key. A Get Attributes request containing the Object
1014 Type attribute name twice is sent, but this operation fails since a single Attribute Name cannot
1015 be specified more than once in a Get Attributes request. The Object Type Attribute is then
1016 requested once, and this request succeeds. Thereafter, the Contact Information Attribute is
1017 modified, with the Attribute Index value of 0 specified. The Name attribute is deleted without
1018 specifying the Attribute Index which succeeds (which would have failed under KMIP-1.0). Finally,
1019 the created key is destroyed.

```
0001 # TIME 0
0002 <RequestMessage>
0003   <RequestHeader>
0004     <ProtocolVersion>
0005       <ProtocolVersionMajor type="Integer" value="1"/>
0006       <ProtocolVersionMinor type="Integer" value="2"/>
0007     </ProtocolVersion>
0008     <BatchCount type="Integer" value="1"/>
0009   </RequestHeader>
0010   <BatchItem>
0011     <Operation type="Enumeration" value="Create"/>
0012     <RequestPayload>
0013       <ObjectType type="Enumeration" value="SymmetricKey"/>
0014       <TemplateAttribute>
0015         <Attribute>
0016           <AttributeName type="TextString" value="Cryptographic
0017           Algorithm"/>
0018           <AttributeValue type="Enumeration" value="AES"/>
0019         </Attribute>
0020         <Attribute>
0021           <AttributeName type="TextString" value="Cryptographic
0022           Length"/>
0023           <AttributeValue type="Integer" value="256"/>
0024         </Attribute>
```


0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="TC-171-12-name1"/>
0030	<NameType type="Enumeration" value="UninterpretedTextString"/>
0031	</AttributeValue>
0032	</Attribute>
0033	<Attribute>
0034	<AttributeName type="TextString" value="Name"/>
0035	<AttributeValue>
0036	<NameValue type="TextString" value="TC-171-12-name2"/>
0037	<NameType type="Enumeration" value="UninterpretedTextString"/>
0038	</AttributeValue>
0039	</Attribute>
0040	<Attribute>
0041	<AttributeName type="TextString" value="Contact Information"/>
0042	<AttributeValue type="TextString" value="admin@localhost"/>
0043	</Attribute>
0044	</TemplateAttribute>
0045	</RequestPayload>
0046	</BatchItem>
0047	</RequestMessage>
0048	<ResponseMessage>
0049	<ResponseHeader>
0050	<ProtocolVersion>
0051	<ProtocolVersionMajor type="Integer" value="1"/>
0052	<ProtocolVersionMinor type="Integer" value="2"/>
0053	</ProtocolVersion>
0054	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0055	<BatchCount type="Integer" value="1"/>
0056	</ResponseHeader>
0057	<BatchItem>
0058	<Operation type="Enumeration" value="Create"/>
0059	<ResultStatus type="Enumeration" value="Success"/>
0060	<ResponsePayload>
0061	<ObjectType type="Enumeration" value="SymmetricKey"/>
0062	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0063	</ResponsePayload>
0064	</BatchItem>
0065	</ResponseMessage>
	# TIME 1
0066	<RequestMessage>
0067	<RequestHeader>
0068	<ProtocolVersion>
0069	<ProtocolVersionMajor type="Integer" value="1"/>
0070	<ProtocolVersionMinor type="Integer" value="2"/>
0071	</ProtocolVersion>

0072	<BatchCount type="Integer" value="1"/>
0073	</RequestHeader>
0074	<BatchItem>
0075	<Operation type="Enumeration" value="GetAttributes"/>
0076	<RequestPayload>
0077	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0078	<AttributeName type="TextString" value="Object Type"/>
0079	<AttributeName type="TextString" value="Object Type"/>
0080	</RequestPayload>
0081	</BatchItem>
0082	</RequestMessage>
0083	<ResponseMessage>
0084	<ResponseHeader>
0085	<ProtocolVersion>
0086	<ProtocolVersionMajor type="Integer" value="1"/>
0087	<ProtocolVersionMinor type="Integer" value="2"/>
0088	</ProtocolVersion>
0089	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0090	<BatchCount type="Integer" value="1"/>
0091	</ResponseHeader>
0092	<BatchItem>
0093	<Operation type="Enumeration" value="GetAttributes"/>
0094	<ResultStatus type="Enumeration" value="OperationFailed"/>
0095	<ResultReason type="Enumeration" value="InvalidMessage"/>
0096	<ResultMessage type="TextString" value="Attribute Name specified
	more than once: Object Type"/>
0097	</BatchItem>
0098	</ResponseMessage>
	# TIME 2
0099	<RequestMessage>
0100	<RequestHeader>
0101	<ProtocolVersion>
0102	<ProtocolVersionMajor type="Integer" value="1"/>
0103	<ProtocolVersionMinor type="Integer" value="2"/>
0104	</ProtocolVersion>
0105	<BatchCount type="Integer" value="1"/>
0106	</RequestHeader>
0107	<BatchItem>
0108	<Operation type="Enumeration" value="GetAttributes"/>
0109	<RequestPayload>
0110	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0111	<AttributeName type="TextString" value="Object Type"/>
0112	</RequestPayload>
0113	</BatchItem>
0114	</RequestMessage>
0115	<ResponseMessage>
0116	<ResponseHeader>
0117	<ProtocolVersion>
0118	<ProtocolVersionMajor type="Integer" value="1"/>
0119	<ProtocolVersionMinor type="Integer" value="2"/>
0120	</ProtocolVersion>
0121	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0122	<BatchCount type="Integer" value="1"/>
0123	</ResponseHeader>

0124	<BatchItem>
0125	<Operation type="Enumeration" value="GetAttributes"/>
0126	<ResultStatus type="Enumeration" value="Success"/>
0127	<ResponsePayload>
0128	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0129	<Attribute>
0130	<AttributeName type="TextString" value="Object Type"/>
0131	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0132	</Attribute>
0133	</ResponsePayload>
0134	</BatchItem>
0135	</ResponseMessage>
	# TIME 3
0136	<RequestMessage>
0137	<RequestHeader>
0138	<ProtocolVersion>
0139	<ProtocolVersionMajor type="Integer" value="1"/>
0140	<ProtocolVersionMinor type="Integer" value="2"/>
0141	</ProtocolVersion>
0142	<BatchCount type="Integer" value="1"/>
0143	</RequestHeader>
0144	<BatchItem>
0145	<Operation type="Enumeration" value="ModifyAttribute"/>
0146	<RequestPayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0148	<Attribute>
0149	<AttributeName type="TextString" value="Contact
	Information"/>
0150	<AttributeIndex type="Integer" value="0"/>
0151	<AttributeValue type="TextString" value="donald@localhost"/>
0152	</Attribute>
0153	</RequestPayload>
0154	</BatchItem>
0155	</RequestMessage>
0156	<ResponseMessage>
0157	<ResponseHeader>
0158	<ProtocolVersion>
0159	<ProtocolVersionMajor type="Integer" value="1"/>
0160	<ProtocolVersionMinor type="Integer" value="2"/>
0161	</ProtocolVersion>
0162	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0163	<BatchCount type="Integer" value="1"/>
0164	</ResponseHeader>
0165	<BatchItem>
0166	<Operation type="Enumeration" value="ModifyAttribute"/>
0167	<ResultStatus type="Enumeration" value="Success"/>
0168	<ResponsePayload>
0169	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0170	<Attribute>
0171	<AttributeName type="TextString" value="Contact
	Information"/>
0172	<AttributeValue type="TextString" value="donald@localhost"/>
0173	</Attribute>
0174	</ResponsePayload>

0175	</BatchItem>
0176	</ResponseMessage>
# TIME 4	
0177	<RequestMessage>
0178	<RequestHeader>
0179	<ProtocolVersion>
0180	<ProtocolVersionMajor type="Integer" value="1"/>
0181	<ProtocolVersionMinor type="Integer" value="2"/>
0182	</ProtocolVersion>
0183	<BatchCount type="Integer" value="1"/>
0184	</RequestHeader>
0185	<BatchItem>
0186	<Operation type="Enumeration" value="DeleteAttribute"/>
0187	<RequestPayload>
0188	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0189	<AttributeName type="TextString" value="Name"/>
0190	</RequestPayload>
0191	</BatchItem>
0192	</RequestMessage>
0193	<ResponseMessage>
0194	<ResponseHeader>
0195	<ProtocolVersion>
0196	<ProtocolVersionMajor type="Integer" value="1"/>
0197	<ProtocolVersionMinor type="Integer" value="2"/>
0198	</ProtocolVersion>
0199	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0200	<BatchCount type="Integer" value="1"/>
0201	</ResponseHeader>
0202	<BatchItem>
0203	<Operation type="Enumeration" value="DeleteAttribute"/>
0204	<ResultStatus type="Enumeration" value="Success"/>
0205	<ResponsePayload>
0206	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0207	<Attribute>
0208	<AttributeName type="TextString" value="Name"/>
0209	<AttributeValue>
0210	<NameValue type="TextString" value="TC-171-12-name1"/>
0211	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0212	</AttributeValue>
0213	</Attribute>
0214	</ResponsePayload>
0215	</BatchItem>
0216	</ResponseMessage>
# TIME 5	
0217	<RequestMessage>
0218	<RequestHeader>
0219	<ProtocolVersion>
0220	<ProtocolVersionMajor type="Integer" value="1"/>
0221	<ProtocolVersionMinor type="Integer" value="2"/>
0222	</ProtocolVersion>
0223	<BatchCount type="Integer" value="1"/>
0224	</RequestHeader>
0225	<BatchItem>

0226	<Operation type="Enumeration" value="Destroy"/>
0227	<RequestPayload>
0228	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0229	</RequestPayload>
0230	</BatchItem>
0231	</RequestMessage>
0232	<ResponseMessage>
0233	<ResponseHeader>
0234	<ProtocolVersion>
0235	<ProtocolVersionMajor type="Integer" value="1"/>
0236	<ProtocolVersionMinor type="Integer" value="2"/>
0237	</ProtocolVersion>
0238	<TimeStamp type="DateTime" value="2012-04-27T08:14:44+00:00"/>
0239	<BatchCount type="Integer" value="1"/>
0240	</ResponseHeader>
0241	<BatchItem>
0242	<Operation type="Enumeration" value="Destroy"/>
0243	<ResultStatus type="Enumeration" value="Success"/>
0244	<ResponsePayload>
0245	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0246	</ResponsePayload>
0247	</BatchItem>
0248	</ResponseMessage>

1020

1021 2.3.35 TC-181-12 - Digests of Symmetric Keys

1022 Exercise the Digest attribute by registering two symmetric keys with the same key material but
1023 using different Key Format Type. The Digest Value for the key with the Key Format Type set to
1024 Transparent Symmetric Key is calculated on the TTLV-encoded Key Material structure, whereas
1025 the Digest Value for the key registered in the Raw Key Format Type is calculated on the raw Key
1026 Material Byte String. The server calculates the value of the mandatory Digest attribute instance
1027 using the Key Format Type used by the client when registering the keys. Thereafter, the client
1028 asks the server to create a symmetric key using the Create operation. In this situation, it is up to
1029 the server to choose what Key Format Type of the created key it uses to calculate the Digest
1030 Value.

1031 Note: This test case assumes a server that does not compute any additional Digest attributes
1032 using another Hashing Algorithm and/or Key Format Type. A server is permitted to provide
1033 multiple Digest attributes.

1034

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>

0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Length"/>
0022	<AttributeValue type="Integer" value="256"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Cryptographic
0026	Usage Mask"/>
0027	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="x-ID"/>
0031	<AttributeValue type="TextString" value="TC-181-12-key1"/>
0032	</Attribute>
0033	</TemplateAttribute>
0034	<SymmetricKey>
0035	<KeyBlock>
0036	<KeyFormatType type="Enumeration" value="Raw"/>
0037	<KeyValue>
0038	<KeyMaterial type="ByteString"
0039	value="0000111122223333444455556666777788889999aaaabbbbccccdddeeeef
0040	fff"/>
0041	</KeyValue>
0042	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0043	<CryptographicLength type="Integer" value="256"/>
0044	</KeyBlock>
0045	</SymmetricKey>
0046	</RequestPayload>
0047	</BatchItem>
0048	</RequestMessage>
0049	<ResponseMessage>
0050	<ResponseHeader>
0051	<ProtocolVersion>
0052	<ProtocolVersionMajor type="Integer" value="1"/>
0053	<ProtocolVersionMinor type="Integer" value="2"/>
0054	</ProtocolVersion>
0055	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0056	<BatchCount type="Integer" value="1"/>
0057	</ResponseHeader>
0058	<BatchItem>
0059	<Operation type="Enumeration" value="Register"/>
0060	<ResultStatus type="Enumeration" value="Success"/>
0061	<ResponsePayload>
0062	<UniqueIdentifier type="TextString"
0063	value="\$UNIQUE_IDENTIFIER_0"/>
0064	</ResponsePayload>

0059	</BatchItem>
0060	</ResponseMessage>
# TIME 1	
0061	<RequestMessage>
0062	<RequestHeader>
0063	<ProtocolVersion>
0064	<ProtocolVersionMajor type="Integer" value="1"/>
0065	<ProtocolVersionMinor type="Integer" value="2"/>
0066	</ProtocolVersion>
0067	<BatchCount type="Integer" value="1"/>
0068	</RequestHeader>
0069	<BatchItem>
0070	<Operation type="Enumeration" value="GetAttributes"/>
0071	<RequestPayload>
0072	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0073	<AttributeName type="TextString" value="Digest"/>
0074	</RequestPayload>
0075	</BatchItem>
0076	</RequestMessage>
0077	<ResponseMessage>
0078	<ResponseHeader>
0079	<ProtocolVersion>
0080	<ProtocolVersionMajor type="Integer" value="1"/>
0081	<ProtocolVersionMinor type="Integer" value="2"/>
0082	</ProtocolVersion>
0083	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0084	<BatchCount type="Integer" value="1"/>
0085	</ResponseHeader>
0086	<BatchItem>
0087	<Operation type="Enumeration" value="GetAttributes"/>
0088	<ResultStatus type="Enumeration" value="Success"/>
0089	<ResponsePayload>
0090	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0091	<Attribute>
0092	<AttributeName type="TextString" value="Digest"/>
0093	<AttributeValue>
0094	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0095	<DigestValue type="ByteString"
	value="6c064fe051add11edc07727b594eb48711df843e08445bba2cd786bc16bc58e8"/>
0096	<KeyFormatType type="Enumeration" value="Raw"/>
0097	</AttributeValue>
0098	</Attribute>
0099	</ResponsePayload>
0100	</BatchItem>
0101	</ResponseMessage>
# TIME 2	
0102	<RequestMessage>
0103	<RequestHeader>
0104	<ProtocolVersion>
0105	<ProtocolVersionMajor type="Integer" value="1"/>
0106	<ProtocolVersionMinor type="Integer" value="2"/>
0107	</ProtocolVersion>
0108	<BatchCount type="Integer" value="1"/>

0109	</RequestHeader>
0110	<BatchItem>
0111	<Operation type="Enumeration" value="Register"/>
0112	<RequestPayload>
0113	<ObjectType type="Enumeration" value="SymmetricKey"/>
0114	<TemplateAttribute>
0115	<Attribute>
0116	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0117	<AttributeValue type="Enumeration" value="AES"/>
0118	</Attribute>
0119	<Attribute>
0120	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0121	<AttributeValue type="Integer" value="256"/>
0122	</Attribute>
0123	<Attribute>
0124	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0125	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0126	</Attribute>
0127	<Attribute>
0128	<AttributeName type="TextString" value="x-ID"/>
0129	<AttributeValue type="TextString" value="TC-181-12-key2"/>
0130	</Attribute>
0131	</TemplateAttribute>
0132	<SymmetricKey>
0133	<KeyBlock>
0134	<KeyFormatType type="Enumeration"
	value="TransparentSymmetricKey"/>
0135	<KeyValue>
0136	<KeyMaterial>
0137	<Key type="ByteString"
	value="0000111122223333444455556666777788889999aaaabbbbccccdddeeeeff
	fff"/>
0138	</KeyMaterial>
0139	</KeyValue>
0140	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0141	<CryptographicLength type="Integer" value="256"/>
0142	</KeyBlock>
0143	</SymmetricKey>
0144	</RequestPayload>
0145	</BatchItem>
0146	</RequestMessage>
0147	<ResponseMessage>
0148	<ResponseHeader>
0149	<ProtocolVersion>
0150	<ProtocolVersionMajor type="Integer" value="1"/>
0151	<ProtocolVersionMinor type="Integer" value="2"/>
0152	</ProtocolVersion>
0153	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0154	<BatchCount type="Integer" value="1"/>
0155	</ResponseHeader>
0156	<BatchItem>
0157	<Operation type="Enumeration" value="Register"/>
0158	<ResultStatus type="Enumeration" value="Success"/>
0159	<ResponsePayload>

0160	<UniqueIdentifier type="TextString"
0161	value="\$UNIQUE_IDENTIFIER_1"/>
0162	</ResponsePayload>
0163	</BatchItem>
0164	</ResponseMessage>
# TIME 3	
0164	<RequestMessage>
0165	<RequestHeader>
0166	<ProtocolVersion>
0167	<ProtocolVersionMajor type="Integer" value="1"/>
0168	<ProtocolVersionMinor type="Integer" value="2"/>
0169	</ProtocolVersion>
0170	<BatchCount type="Integer" value="1"/>
0171	</RequestHeader>
0172	<BatchItem>
0173	<Operation type="Enumeration" value="GetAttributes"/>
0174	<RequestPayload>
0175	<UniqueIdentifier type="TextString"
0176	value="\$UNIQUE_IDENTIFIER_1"/>
0177	<AttributeName type="TextString" value="Digest"/>
0178	</RequestPayload>
0179	</BatchItem>
0180	</RequestMessage>
0181	<ResponseMessage>
0182	<ResponseHeader>
0183	<ProtocolVersion>
0184	<ProtocolVersionMajor type="Integer" value="1"/>
0185	<ProtocolVersionMinor type="Integer" value="2"/>
0186	</ProtocolVersion>
0187	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0188	<BatchCount type="Integer" value="1"/>
0189	</ResponseHeader>
0190	<BatchItem>
0191	<Operation type="Enumeration" value="GetAttributes"/>
0192	<ResultStatus type="Enumeration" value="Success"/>
0193	<ResponsePayload>
0194	<UniqueIdentifier type="TextString"
0195	value="\$UNIQUE_IDENTIFIER_1"/>
0196	<Attribute>
0197	<AttributeName type="TextString" value="Digest"/>
0198	<AttributeValue>
0199	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0200	<DigestValue type="ByteString"
0201	value="499ce96ff6f5e19fe9fe7a2fe4c3e92b88db0001a4e8df28d9966856b6c4b87c"/>
0202	<KeyFormatType type="Enumeration"
0203	value="TransparentSymmetricKey"/>
0204	</Attribute>
0205	</BatchItem>
0206	</ResponsePayload>
0207	</BatchItem>
0208	</ResponseMessage>
# TIME 4	
0205	<RequestMessage>
0206	<RequestHeader>
0207	<ProtocolVersion>

0208	<ProtocolVersionMajor type="Integer" value="1"/>
0209	<ProtocolVersionMinor type="Integer" value="2"/>
0210	</ProtocolVersion>
0211	<BatchCount type="Integer" value="1"/>
0212	</RequestHeader>
0213	<BatchItem>
0214	<Operation type="Enumeration" value="Create"/>
0215	<RequestPayload>
0216	<ObjectType type="Enumeration" value="SymmetricKey"/>
0217	<TemplateAttribute>
0218	<Attribute>
0219	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0220	<AttributeValue type="Enumeration" value="AES"/>
0221	</Attribute>
0222	<Attribute>
0223	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0224	<AttributeValue type="Integer" value="256"/>
0225	</Attribute>
0226	<Attribute>
0227	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0228	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0229	</Attribute>
0230	<Attribute>
0231	<AttributeName type="TextString" value="x-ID"/>
0232	<AttributeValue type="TextString" value="TC-181-12-key3"/>
0233	</Attribute>
0234	</TemplateAttribute>
0235	</RequestPayload>
0236	</BatchItem>
0237	</RequestMessage>
0238	<ResponseMessage>
0239	<ResponseHeader>
0240	<ProtocolVersion>
0241	<ProtocolVersionMajor type="Integer" value="1"/>
0242	<ProtocolVersionMinor type="Integer" value="2"/>
0243	</ProtocolVersion>
0244	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0245	<BatchCount type="Integer" value="1"/>
0246	</ResponseHeader>
0247	<BatchItem>
0248	<Operation type="Enumeration" value="Create"/>
0249	<ResultStatus type="Enumeration" value="Success"/>
0250	<ResponsePayload>
0251	<ObjectType type="Enumeration" value="SymmetricKey"/>
0252	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0253	</ResponsePayload>
0254	</BatchItem>
0255	</ResponseMessage>
	# TIME 5
0256	<RequestMessage>
0257	<RequestHeader>
0258	<ProtocolVersion>
0259	<ProtocolVersionMajor type="Integer" value="1"/>

0260	<ProtocolVersionMinor type="Integer" value="2"/>
0261	</ProtocolVersion>
0262	<BatchCount type="Integer" value="1"/>
0263	</RequestHeader>
0264	<BatchItem>
0265	<Operation type="Enumeration" value="GetAttributes"/>
0266	<RequestPayload>
0267	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0268	<AttributeName type="TextString" value="Digest"/>
0269	</RequestPayload>
0270	</BatchItem>
0271	</RequestMessage>
0272	<ResponseMessage>
0273	<ResponseHeader>
0274	<ProtocolVersion>
0275	<ProtocolVersionMajor type="Integer" value="1"/>
0276	<ProtocolVersionMinor type="Integer" value="2"/>
0277	</ProtocolVersion>
0278	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0279	<BatchCount type="Integer" value="1"/>
0280	</ResponseHeader>
0281	<BatchItem>
0282	<Operation type="Enumeration" value="GetAttributes"/>
0283	<ResultStatus type="Enumeration" value="Success"/>
0284	<ResponsePayload>
0285	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0286	<Attribute>
0287	<AttributeName type="TextString" value="Digest"/>
0288	<AttributeValue>
0289	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0290	<DigestValue type="ByteString"
	value="314b223505091db03325c638a6016cf7080d3b116eb3f4896b6d24d4ec2215f8"/>
0291	<KeyFormatType type="Enumeration" value="Raw"/>
0292	</AttributeValue>
0293	</Attribute>
0294	</ResponsePayload>
0295	</BatchItem>
0296	</ResponseMessage>
	# TIME 6
0297	<RequestMessage>
0298	<RequestHeader>
0299	<ProtocolVersion>
0300	<ProtocolVersionMajor type="Integer" value="1"/>
0301	<ProtocolVersionMinor type="Integer" value="2"/>
0302	</ProtocolVersion>
0303	<BatchCount type="Integer" value="1"/>
0304	</RequestHeader>
0305	<BatchItem>
0306	<Operation type="Enumeration" value="Get"/>
0307	<RequestPayload>
0308	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0309	<KeyFormatType type="Enumeration" value="Raw"/>
0310	</RequestPayload>

0311	</BatchItem>
0312	</RequestMessage>
0313	<ResponseMessage>
0314	<ResponseHeader>
0315	<ProtocolVersion>
0316	<ProtocolVersionMajor type="Integer" value="1"/>
0317	<ProtocolVersionMinor type="Integer" value="2"/>
0318	</ProtocolVersion>
0319	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0320	<BatchCount type="Integer" value="1"/>
0321	</ResponseHeader>
0322	<BatchItem>
0323	<Operation type="Enumeration" value="Get"/>
0324	<ResultStatus type="Enumeration" value="Success"/>
0325	<ResponsePayload>
0326	<ObjectType type="Enumeration" value="SymmetricKey"/>
0327	<UniqueIdentifier type="TextString"
0328	value="\$UNIQUE_IDENTIFIER_2"/>
0329	<SymmetricKey>
0330	<KeyBlock>
0331	<KeyFormatType type="Enumeration" value="Raw"/>
0332	<KeyValue>
0333	<KeyMaterial type="ByteString"
0334	value="c1a99ac4716d4ea787d40b449d7b816f0ce82772b463cbf3a042b3f8e81e7
0335	bb7"/>
0336	</KeyValue>
0337	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0338	<CryptographicLength type="Integer" value="256"/>
0339	</KeyBlock>
0340	</SymmetricKey>
0341	</ResponsePayload>
0342	</BatchItem>
0343	</ResponseMessage>
# TIME 7	
0341	<RequestMessage>
0342	<RequestHeader>
0343	<ProtocolVersion>
0344	<ProtocolVersionMajor type="Integer" value="1"/>
0345	<ProtocolVersionMinor type="Integer" value="2"/>
0346	</ProtocolVersion>
0347	<BatchCount type="Integer" value="1"/>
0348	</RequestHeader>
0349	<BatchItem>
0350	<Operation type="Enumeration" value="Destroy"/>
0351	<RequestPayload>
0352	<UniqueIdentifier type="TextString"
0353	value="\$UNIQUE_IDENTIFIER_0"/>
0354	</RequestPayload>
0355	</BatchItem>
0356	</RequestMessage>
0357	<ResponseMessage>
0358	<ResponseHeader>
0359	<ProtocolVersion>
0360	<ProtocolVersionMajor type="Integer" value="1"/>
0361	<ProtocolVersionMinor type="Integer" value="2"/>
0361	</ProtocolVersion>

0362	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0363	<BatchCount type="Integer" value="1"/>
0364	</ResponseHeader>
0365	<BatchItem>
0366	<Operation type="Enumeration" value="Destroy"/>
0367	<ResultStatus type="Enumeration" value="Success"/>
0368	<ResponsePayload>
0369	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0370	</ResponsePayload>
0371	</BatchItem>
0372	</ResponseMessage>
# TIME 8	
0373	<RequestMessage>
0374	<RequestHeader>
0375	<ProtocolVersion>
0376	<ProtocolVersionMajor type="Integer" value="1"/>
0377	<ProtocolVersionMinor type="Integer" value="2"/>
0378	</ProtocolVersion>
0379	<BatchCount type="Integer" value="1"/>
0380	</RequestHeader>
0381	<BatchItem>
0382	<Operation type="Enumeration" value="Destroy"/>
0383	<RequestPayload>
0384	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0385	</RequestPayload>
0386	</BatchItem>
0387	</RequestMessage>
0388	<ResponseMessage>
0389	<ResponseHeader>
0390	<ProtocolVersion>
0391	<ProtocolVersionMajor type="Integer" value="1"/>
0392	<ProtocolVersionMinor type="Integer" value="2"/>
0393	</ProtocolVersion>
0394	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0395	<BatchCount type="Integer" value="1"/>
0396	</ResponseHeader>
0397	<BatchItem>
0398	<Operation type="Enumeration" value="Destroy"/>
0399	<ResultStatus type="Enumeration" value="Success"/>
0400	<ResponsePayload>
0401	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0402	</ResponsePayload>
0403	</BatchItem>
0404	</ResponseMessage>
# TIME 9	
0405	<RequestMessage>
0406	<RequestHeader>
0407	<ProtocolVersion>
0408	<ProtocolVersionMajor type="Integer" value="1"/>
0409	<ProtocolVersionMinor type="Integer" value="2"/>
0410	</ProtocolVersion>
0411	<BatchCount type="Integer" value="1"/>
0412	</RequestHeader>

0413	<BatchItem>
0414	<Operation type="Enumeration" value="Destroy"/>
0415	<RequestPayload>
0416	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0417	</RequestPayload>
0418	</BatchItem>
0419	</RequestMessage>
0420	<ResponseMessage>
0421	<ResponseHeader>
0422	<ProtocolVersion>
0423	<ProtocolVersionMajor type="Integer" value="1"/>
0424	<ProtocolVersionMinor type="Integer" value="2"/>
0425	</ProtocolVersion>
0426	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0427	<BatchCount type="Integer" value="1"/>
0428	</ResponseHeader>
0429	<BatchItem>
0430	<Operation type="Enumeration" value="Destroy"/>
0431	<ResultStatus type="Enumeration" value="Success"/>
0432	<ResponsePayload>
0433	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0434	</ResponsePayload>
0435	</BatchItem>
0436	</ResponseMessage>

1035

1036 2.3.36 TC-182-12 - Digests of RSA Private Keys

1037 Exercise the Digest attribute by registering two RSA private keys with the same key material but
1038 using different Key Format Type. The Digest Value for the key with the Key Format Type set to
1039 Transparent RSA Private Key is calculated on the TTLV-encoded Key Material structure, whereas
1040 the Digest Value for the key registered in the PKCS_1 Key Format Type is calculated on the Key
1041 Material Byte String. The server calculates the value of the mandatory Digest attribute instance
1042 using the Key Format Type used by the client when registering the keys.

1043 Note: This test case assumes a server that does not compute any additional Digest attributes
1044 using another Hashing Algorithm and/or Key Format Type. A server is permitted to provide
1045 multiple Digest attributes.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="PrivateKey"/>

```
0013     <TemplateAttribute>
0014         <Attribute>
0015             <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0016             <AttributeValue type="Enumeration" value="RSA"/>
0017         </Attribute>
0018     </Attribute>
0019     <AttributeName type="TextString" value="Cryptographic
Length"/>
0020     <AttributeValue type="Integer" value="2048"/>
0021 </Attribute>
0022 <Attribute>
0023     <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0024     <AttributeValue type="Integer" value="Sign"/>
0025 </Attribute>
0026 <Attribute>
0027     <AttributeName type="TextString" value="x-ID"/>
0028     <AttributeValue type="TextString" value="TC-182-12-
prikey1"/>
0029 </Attribute>
0030 </TemplateAttribute>
0031 <PrivateKey>
0032     <KeyBlock>
0033         <KeyFormatType type="Enumeration" value="PKCS_1"/>
0034         <KeyMaterial type="ByteString"
0035             value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353
57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483
46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa
2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650
89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c
795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f
91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281
5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050
203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a
7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f
a74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b
2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0
e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a
a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e
3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78
965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8
c3cdc2464744a793713dafb9f1dbc799ff96423fecdc3ba794286bce920f4b5c183f
99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967
4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c
ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064
b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e
59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4
990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766
b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab
7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0
e94ad1ee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db
e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa
e1ebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2
7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eaeaf922fd75d5b16b1a5
61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a72
```

0036	6a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d349417e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f8129c32341a8b44f"/>
0037	</KeyValue>
0038	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0039	<CryptographicLength type="Integer" value="2048"/>
0040	</KeyBlock>
0041	</PrivateKey>
0042	</RequestPayload>
0043	</BatchItem>
0044	</RequestMessage>
0045	<ResponseMessage>
0046	<ResponseHeader>
0047	<ProtocolVersion>
0048	<ProtocolVersionMajor type="Integer" value="1"/>
0049	<ProtocolVersionMinor type="Integer" value="2"/>
0050	</ProtocolVersion>
0051	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0052	<BatchCount type="Integer" value="1"/>
0053	</ResponseHeader>
0054	<BatchItem>
0055	<Operation type="Enumeration" value="Register"/>
0056	<ResultStatus type="Enumeration" value="Success"/>
0057	<ResponsePayload>
0058	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0059	</ResponsePayload>
0060	</BatchItem>
0061	</ResponseMessage>
0062	# TIME 1
0063	<RequestMessage>
0064	<RequestHeader>
0065	<ProtocolVersion>
0066	<ProtocolVersionMajor type="Integer" value="1"/>
0067	<ProtocolVersionMinor type="Integer" value="2"/>
0068	</ProtocolVersion>
0069	<BatchCount type="Integer" value="1"/>
0070	</RequestHeader>
0071	<BatchItem>
0072	<Operation type="Enumeration" value="GetAttributes"/>
0073	<RequestPayload>
0074	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0075	<AttributeName type="TextString" value="Digest"/>
0076	</RequestPayload>
0077	</BatchItem>
0078	</RequestMessage>
0079	<ResponseMessage>
0080	<ResponseHeader>
0081	<ProtocolVersion>
0082	<ProtocolVersionMajor type="Integer" value="1"/>
	<ProtocolVersionMinor type="Integer" value="2"/>
	</ProtocolVersion>

0083	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0084	<BatchCount type="Integer" value="1"/>
0085	</ResponseHeader>
0086	<BatchItem>
0087	<Operation type="Enumeration" value="GetAttributes"/>
0088	<ResultStatus type="Enumeration" value="Success"/>
0089	<ResponsePayload>
0090	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0091	<Attribute>
0092	<AttributeName type="TextString" value="Digest"/>
0093	<AttributeValue>
0094	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0095	<DigestValue type="ByteString"
	value="11110a01ed4589d9987c9ad60368e2b762f2b20c00946e1932c1605a18172f55"/>
0096	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0097	</AttributeValue>
0098	</Attribute>
0099	</ResponsePayload>
0100	</BatchItem>
0101	</ResponseMessage>
	# TIME 2
0102	<RequestMessage>
0103	<RequestHeader>
0104	<ProtocolVersion>
0105	<ProtocolVersionMajor type="Integer" value="1"/>
0106	<ProtocolVersionMinor type="Integer" value="2"/>
0107	</ProtocolVersion>
0108	<BatchCount type="Integer" value="1"/>
0109	</RequestHeader>
0110	<BatchItem>
0111	<Operation type="Enumeration" value="Register"/>
0112	<RequestPayload>
0113	<ObjectType type="Enumeration" value="PrivateKey"/>
0114	<TemplateAttribute>
0115	<Attribute>
0116	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0117	<AttributeValue type="Enumeration" value="RSA"/>
0118	</Attribute>
0119	<Attribute>
0120	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0121	<AttributeValue type="Integer" value="2048"/>
0122	</Attribute>
0123	<Attribute>
0124	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0125	<AttributeValue type="Integer" value="Sign"/>
0126	</Attribute>
0127	<Attribute>
0128	<AttributeName type="TextString" value="x-ID"/>
0129	<AttributeValue type="TextString" value="TC-182-12-
	prikey2"/>
0130	</Attribute>
0131	</TemplateAttribute>

0132	<PrivateKey>
0133	<KeyBlock>
0134	<KeyFormatType type="Enumeration"
	value="TransparentRSAPrivateKey"/>
0135	<KeyValue>
0136	<KeyMaterial>
0137	<Modulus type="BigInteger"
	value="0000000000000000ab7f161c0042496ccd6c6d4dad919973435357776003
	acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b8d
	71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89b9
	bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f98135
	b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328ab
	f70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013da
	809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612a2
	9a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f605"/>
0138	<PrivateExponent type="BigInteger"
	value="3b12455d53c1816516c518493f6398aafa72b17dfa894db888a7d48c0a47f
	62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618fa74cde5fda
	fabdb6aa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b2144d2b722
	93e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0e8fef17c37
	542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0aa49ce816e5
	be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e3806ad982d
	1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78965c2aed48
	77ba3917df07c5e927474f19e764ba61dc38d63bf29"/>
0139	<PublicExponent type="BigInteger"
	value="0000000000010001"/>
0140	<P type="BigInteger"
	value="000000000000000d5c69c8c3cdc2464744a793713dafb9f1dbc799ff9642
	3fecdc3ba794286bce920f4b5c183f99ee9028db6212c6277c4c8297fcfbce7f7c24
	ca4c51fc7182fb8f4019fb1d5659674c5cbe6d5fa992051341760cd00735729a070a
	9e54d342beba8ef47ee82d3a01b04cec4a00d4ddb41e35116fc221e854b43a696c0e
	6419b1b"/>
0141	<Q type="BigInteger"
	value="000000000000000cd5ea7702789064b673540cbff09356ad80bc3d592812
	eba47610b9fac6aecefe22acae438459cda74e59653d88c04189d34399bf5b14b920
	e34ef38a7d09fe69593396e8fe735e6f0a6ae4990401041d8a406b6fd86a1161e45f
	95a3eaa5c1012e6662e44f15f335ac971e1766b2bb9c985109974141b44d37e1e319
	820a55f"/>
0142	<PrimeExponentP type="BigInteger"
	value="000000000000000b2871237bf9fad38c3316ab7877a6a868063e542a7186
	d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0e94ad1ee82158108fbc866
	4517a5a467fb963014bd5dcc2b4fb087c23039d11920dbe22fd9f16b4d89e23225cd
	455adbaf32ef43f185864a36d630309d6853f7714b39aae1ebee3938f87c2707e178
	c739f9f"/>
0143	<PrimeExponentQ type="BigInteger"
	value="0000000000000009690bed14b2afaa26d986d592231ee27d71d49065bd2b
	a1f78157e20229881fd9d23227d0f8479eaeafa922fd75d5b16b1a561fa6680b040ca
	0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bffa85a726a1d90260e4f10
	84f518234dcd3fe770b9520215bd543bb6a4117718754676a34171666a79f26e79c1
	49c5aa1"/>
0144	<CRTCoefficient type="BigInteger"
	value="000000000000000a0c985a0a0a791a659f99731134c44f37b2e520a2cea3
	5800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a1cac91
	011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d349417e1f0c
	9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f8129c3234
	1a8b44f"/>
0145	</KeyMaterial>

0146	</KeyValue>
0147	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0148	<CryptographicLength type="Integer" value="2048"/>
0149	</KeyBlock>
0150	</PrivateKey>
0151	</RequestPayload>
0152	</BatchItem>
0153	</RequestMessage>
0154	<ResponseMessage>
0155	<ResponseHeader>
0156	<ProtocolVersion>
0157	<ProtocolVersionMajor type="Integer" value="1"/>
0158	<ProtocolVersionMinor type="Integer" value="2"/>
0159	</ProtocolVersion>
0160	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0161	<BatchCount type="Integer" value="1"/>
0162	</ResponseHeader>
0163	<BatchItem>
0164	<Operation type="Enumeration" value="Register"/>
0165	<ResultStatus type="Enumeration" value="Success"/>
0166	<ResponsePayload>
0167	<UniqueIdentifier type="TextString"
0168	value="\$UNIQUE_IDENTIFIER_1"/>
0169	</ResponsePayload>
0170	</BatchItem>
0170	</ResponseMessage>
0171	# TIME 3
0171	<RequestMessage>
0172	<RequestHeader>
0173	<ProtocolVersion>
0174	<ProtocolVersionMajor type="Integer" value="1"/>
0175	<ProtocolVersionMinor type="Integer" value="2"/>
0176	</ProtocolVersion>
0177	<BatchCount type="Integer" value="1"/>
0178	</RequestHeader>
0179	<BatchItem>
0180	<Operation type="Enumeration" value="GetAttributes"/>
0181	<RequestPayload>
0182	<UniqueIdentifier type="TextString"
0183	value="\$UNIQUE_IDENTIFIER_1"/>
0184	<AttributeName type="TextString" value="Digest"/>
0185	</RequestPayload>
0186	</BatchItem>
0186	</RequestMessage>
0187	<ResponseMessage>
0188	<ResponseHeader>
0189	<ProtocolVersion>
0190	<ProtocolVersionMajor type="Integer" value="1"/>
0191	<ProtocolVersionMinor type="Integer" value="2"/>
0192	</ProtocolVersion>
0193	<TimeStamp type="DateTime" value="2012-04-27T08:14:45+00:00"/>
0194	<BatchCount type="Integer" value="1"/>
0195	</ResponseHeader>
0196	<BatchItem>
0197	<Operation type="Enumeration" value="GetAttributes"/>
0198	<ResultStatus type="Enumeration" value="Success"/>

0199	<ResponsePayload>
0200	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0201	<Attribute>
0202	<AttributeName type="TextString" value="Digest"/>
0203	<AttributeValue>
0204	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0205	<DigestValue type="ByteString"
	value="d73bbc51e83332935f912dbfc35c5efc3b7bf8021835ba86b8da4181f74244ac"/>
0206	<KeyFormatType type="Enumeration"
	value="TransparentRSAPrivateKey"/>
0207	</AttributeValue>
0208	</Attribute>
0209	</ResponsePayload>
0210	</BatchItem>
0211	</ResponseMessage>
	# TIME 4
0212	<RequestMessage>
0213	<RequestHeader>
0214	<ProtocolVersion>
0215	<ProtocolVersionMajor type="Integer" value="1"/>
0216	<ProtocolVersionMinor type="Integer" value="2"/>
0217	</ProtocolVersion>
0218	<BatchCount type="Integer" value="1"/>
0219	</RequestHeader>
0220	<BatchItem>
0221	<Operation type="Enumeration" value="Destroy"/>
0222	<RequestPayload>
0223	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0224	</RequestPayload>
0225	</BatchItem>
0226	</RequestMessage>
0227	<ResponseMessage>
0228	<ResponseHeader>
0229	<ProtocolVersion>
0230	<ProtocolVersionMajor type="Integer" value="1"/>
0231	<ProtocolVersionMinor type="Integer" value="2"/>
0232	</ProtocolVersion>
0233	<TimeStamp type="DateTime" value="2012-04-27T08:14:46+00:00"/>
0234	<BatchCount type="Integer" value="1"/>
0235	</ResponseHeader>
0236	<BatchItem>
0237	<Operation type="Enumeration" value="Destroy"/>
0238	<ResultStatus type="Enumeration" value="Success"/>
0239	<ResponsePayload>
0240	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0241	</ResponsePayload>
0242	</BatchItem>
0243	</ResponseMessage>
	# TIME 5
0244	<RequestMessage>
0245	<RequestHeader>
0246	<ProtocolVersion>

0247	<ProtocolVersionMajor type="Integer" value="1"/>
0248	<ProtocolVersionMinor type="Integer" value="2"/>
0249	</ProtocolVersion>
0250	<BatchCount type="Integer" value="1"/>
0251	</RequestHeader>
0252	<BatchItem>
0253	<Operation type="Enumeration" value="Destroy"/>
0254	<RequestPayload>
0255	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0256	</RequestPayload>
0257	</BatchItem>
0258	</RequestMessage>
0259	<ResponseMessage>
0260	<ResponseHeader>
0261	<ProtocolVersion>
0262	<ProtocolVersionMajor type="Integer" value="1"/>
0263	<ProtocolVersionMinor type="Integer" value="2"/>
0264	</ProtocolVersion>
0265	<TimeStamp type="DateTime" value="2012-04-27T08:14:46+00:00"/>
0266	<BatchCount type="Integer" value="1"/>
0267	</ResponseHeader>
0268	<BatchItem>
0269	<Operation type="Enumeration" value="Destroy"/>
0270	<ResultStatus type="Enumeration" value="Success"/>
0271	<ResponsePayload>
0272	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0273	</ResponsePayload>
0274	</BatchItem>
0275	</ResponseMessage>

1046

1047 2.3.37 TC-NP-1-12 - Put

1048 In this test case the client issues a Create request, whereby the server creates a new symmetric
1049 key and returns the Unique Identifier. To clean up, the client then performs a Destroy operation
1050 to destroy the key.

1051 The server sends Put messages to the client via a separate channel.

1052

	# TIME 0
	# [Client-to-Server]
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>

0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="x-ID"/>
0028	<AttributeValue type="TextString" value="TC-NP-1-12"/>
0029	</Attribute>
0030	</TemplateAttribute>
0031	</RequestPayload>
0032	</BatchItem>
0033	</RequestMessage>
# [Client-to-Server]	
0034	<ResponseMessage>
0035	<ResponseHeader>
0036	<ProtocolVersion>
0037	<ProtocolVersionMajor type="Integer" value="1"/>
0038	<ProtocolVersionMinor type="Integer" value="2"/>
0039	</ProtocolVersion>
0040	<TimeStamp type="DateTime" value="2013-06-26T05:13:47+00:00"/>
0041	<BatchCount type="Integer" value="1"/>
0042	</ResponseHeader>
0043	<BatchItem>
0044	<Operation type="Enumeration" value="Create"/>
0045	<ResultStatus type="Enumeration" value="Success"/>
0046	<ResponsePayload>
0047	<ObjectType type="Enumeration" value="SymmetricKey"/>
0048	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0049	</ResponsePayload>
0050	</BatchItem>
0051	</ResponseMessage>
# TIME 1	
# [Server-to-Client]	
0052	<RequestMessage>
0053	<RequestHeader>
0054	<ProtocolVersion>
0055	<ProtocolVersionMajor type="Integer" value="1"/>
0056	<ProtocolVersionMinor type="Integer" value="2"/>
0057	</ProtocolVersion>
0058	<BatchCount type="Integer" value="1"/>
0059	</RequestHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="Put"/>

```

0062     <RequestPayload>
0063         <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0064         <PutFunction type="Enumeration" value="New"/>
0065         <SymmetricKey>
0066             <KeyBlock>
0067                 <KeyFormatType type="Enumeration" value="Raw"/>
0068                 <KeyValue>
0069                     <KeyMaterial type="ByteString"
value="7546ef6cd37c49806824984477987d1e"/>
0070                 </KeyValue>
0071                 <CryptographicAlgorithm type="Enumeration" value="AES"/>
0072                 <CryptographicLength type="Integer" value="128"/>
0073             </KeyBlock>
0074         </SymmetricKey>
0075         <Attribute>
0076             <AttributeName type="TextString" value="x-ID"/>
0077             <AttributeValue type="TextString" value="TC-NP-1-12"/>
0078         </Attribute>
0079         <Attribute>
0080             <AttributeName type="TextString" value="Unique Identifier"/>
0081             <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0082         </Attribute>
0083         <Attribute>
0084             <AttributeName type="TextString" value="Object Type"/>
0085             <AttributeValue type="Enumeration" value="SymmetricKey"/>
0086         </Attribute>
0087         <Attribute>
0088             <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0089             <AttributeValue type="Enumeration" value="AES"/>
0090         </Attribute>
0091         <Attribute>
0092             <AttributeName type="TextString" value="Cryptographic
Length"/>
0093             <AttributeValue type="Integer" value="128"/>
0094         </Attribute>
0095         <Attribute>
0096             <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0097             <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0098         </Attribute>
0099         <Attribute>
0100             <AttributeName type="TextString" value="Digest"/>
0101             <AttributeValue>
0102                 <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0103                 <DigestValue type="ByteString"
value="7549ecda2cd1569974c3748f223fbc947ce9cabce581497522e4b75e9d6ed
e81"/>
0104             <KeyFormatType type="Enumeration" value="Raw"/>
0105             </AttributeValue>
0106         </Attribute>
0107         <Attribute>
0108             <AttributeName type="TextString" value="Fresh"/>
0109             <AttributeValue type="Boolean" value="true"/>
0110         </Attribute>

```

0111	<Attribute>
0112	<AttributeName type="TextString" value="Initial Date"/>
0113	<AttributeValue type="DateTime" value="2013-06-26T05:13:48+00:00"/>
0114	</Attribute>
0115	<Attribute>
0116	<AttributeName type="TextString" value="Last Change Date"/>
0117	<AttributeValue type="DateTime" value="2013-06-26T05:13:48+00:00"/>
0118	</Attribute>
0119	<Attribute>
0120	<AttributeName type="TextString" value="Lease Time"/>
0121	<AttributeValue type="Interval" value="3600"/>
0122	</Attribute>
0123	<Attribute>
0124	<AttributeName type="TextString" value="Original Creation Date"/>
0125	<AttributeValue type="DateTime" value="2013-06-26T05:13:48+00:00"/>
0126	</Attribute>
0127	<Attribute>
0128	<AttributeName type="TextString" value="State"/>
0129	<AttributeValue type="Enumeration" value="PreActive"/>
0130	</Attribute>
0131	</RequestPayload>
0132	</BatchItem>
0133	</RequestMessage>
	# [Server-to-Client]
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="2"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2013-06-26T05:13:48+00:00"/>
0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="Put"/>
0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	</ResponsePayload>
0148	</BatchItem>
0149	</ResponseMessage>
	# TIME 2
	# [Client-to-Server]
0150	<RequestMessage>
0151	<RequestHeader>
0152	<ProtocolVersion>
0153	<ProtocolVersionMajor type="Integer" value="1"/>
0154	<ProtocolVersionMinor type="Integer" value="2"/>
0155	</ProtocolVersion>
0156	<BatchCount type="Integer" value="1"/>
0157	</RequestHeader>
0158	<BatchItem>
0159	<Operation type="Enumeration" value="Destroy"/>
0160	<RequestPayload>

0161	<UniqueIdentifier type="TextString"
0162	value="\$UNIQUE_IDENTIFIER_0"/>
0163	</RequestPayload>
0164	</BatchItem>
	</RequestMessage>
	# [Client-to-Server]
0165	<ResponseMessage>
0166	<ResponseHeader>
0167	<ProtocolVersion>
0168	<ProtocolVersionMajor type="Integer" value="1"/>
0169	<ProtocolVersionMinor type="Integer" value="2"/>
0170	</ProtocolVersion>
0171	<TimeStamp type="DateTime" value="2013-06-26T05:13:48+00:00"/>
0172	<BatchCount type="Integer" value="1"/>
0173	</ResponseHeader>
0174	<BatchItem>
0175	<Operation type="Enumeration" value="Destroy"/>
0176	<ResultStatus type="Enumeration" value="Success"/>
0177	<ResponsePayload>
0178	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0179	</ResponsePayload>
0180	</BatchItem>
0181	</ResponseMessage>

1053

1054 2.3.38 TC-NP-2-12 - Notify & Put

1055 This test case tests the import of key using the Register operation. To validate that the
1056 registered key is treated the same as a locally created key, an attribute is added to the key and
1057 then modified. Finally, the key is destroyed.

1058 The server sends Notify and Put messages to the client via a separate channel.

	# TIME 0
	# [Client-to-Server]
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0016	<AttributeValue type="Integer" value="Encrypt"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>

0020	<AttributeValue type="TextString" value="TC-NP-2-12"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<SymmetricKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="Raw"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString"
	value="1122456789abcdef0123456789abcdef"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0030	<CryptographicLength type="Integer" value="128"/>
0031	</KeyBlock>
0032	</SymmetricKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
	# [Client-to-Server]
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="2"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
	# [Server-to-Client]
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="0"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Put"/>
0063	<RequestPayload>
0064	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0065	<PutFunction type="Enumeration" value="New"/>
0066	<SymmetricKey>
0067	<KeyBlock>
0068	<KeyFormatType type="Enumeration" value="Raw"/>
0069	<KeyValue>
0070	<KeyMaterial type="ByteString"

0071	value="1122456789abcdef0123456789abcdef"/>
0072	</KeyValue>
0073	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0074	<CryptographicLength type="Integer" value="128"/>
0075	</KeyBlock>
0076	</SymmetricKey>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-NP-2-12"/>
0080	</Attribute>
0081	<Attribute>
0082	<AttributeName type="TextString" value="Unique Identifier"/>
0083	<AttributeValue type="TextString"
0084	value="\$UNIQUE_IDENTIFIER_0"/>
0085	</Attribute>
0086	<Attribute>
0087	<AttributeName type="TextString" value="Object Type"/>
0088	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0089	</Attribute>
0090	<Attribute>
0091	<AttributeName type="TextString" value="Cryptographic
0092	Algorithm"/>
0093	<AttributeValue type="Enumeration" value="AES"/>
0094	</Attribute>
0095	<Attribute>
0096	<AttributeName type="TextString" value="Cryptographic
0097	Length"/>
0098	<AttributeValue type="Integer" value="128"/>
0099	</Attribute>
0100	<Attribute>
0101	<AttributeName type="TextString" value="Cryptographic Usage
0102	Mask"/>
0103	<AttributeValue type="Integer" value="Encrypt"/>
0104	</Attribute>
0105	<Attribute>
0106	<AttributeName type="TextString" value="Digest"/>
0107	<AttributeValue>
0108	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0109	<DigestValue type="ByteString"
0110	value="47c01d3851ce2f254d18928526b6126de30cef9a34a4cfbd4648ec3ed21a9
0111	e86"/>
0112	<KeyFormatType type="Enumeration" value="Raw"/>
0113	</AttributeValue>
0114	</Attribute>
0115	<Attribute>
0116	<AttributeName type="TextString" value="Fresh"/>
0117	<AttributeValue type="Boolean" value="true"/>
0118	</Attribute>
0119	<Attribute>
0120	<AttributeName type="TextString" value="Initial Date"/>
0121	<AttributeValue type="DateTime" value="2013-06-
0122	26T05:54:18+00:00"/>
0123	</Attribute>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Last Change Date"/>
0126	<AttributeValue type="DateTime" value="2013-06-
0127	26T05:54:18+00:00"/>

0119	</Attribute>
0120	<Attribute>
0121	<AttributeName type="TextString" value="Lease Time"/>
0122	<AttributeValue type="Interval" value="3600"/>
0123	</Attribute>
0124	<Attribute>
0125	<AttributeName type="TextString" value="State"/>
0126	<AttributeValue type="Enumeration" value="PreActive"/>
0127	</Attribute>
0128	</RequestPayload>
0129	</BatchItem>
0130	</RequestMessage>
0131	# [Server-to-Client]
0132	<ResponseMessage>
0133	<ResponseHeader>
0134	<ProtocolVersion>
0135	<ProtocolVersionMajor type="Integer" value="1"/>
0136	<ProtocolVersionMinor type="Integer" value="0"/>
0137	</ProtocolVersion>
0138	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0139	<BatchCount type="Integer" value="1"/>
0140	</ResponseHeader>
0141	<BatchItem>
0142	<Operation type="Enumeration" value="Put"/>
0143	<ResultStatus type="Enumeration" value="Success"/>
0144	<ResponsePayload>
0145	</ResponsePayload>
0146	</BatchItem>
0147	</ResponseMessage>
0148	# TIME 2
0149	# [Client-to-Server]
0150	<RequestMessage>
0151	<RequestHeader>
0152	<ProtocolVersion>
0153	<ProtocolVersionMajor type="Integer" value="1"/>
0154	<ProtocolVersionMinor type="Integer" value="2"/>
0155	</ProtocolVersion>
0156	<BatchCount type="Integer" value="1"/>
0157	</RequestHeader>
0158	<BatchItem>
0159	<Operation type="Enumeration" value="AddAttribute"/>
0160	<RequestPayload>
0161	<UniqueIdentifier type="TextString"
0162	value="\$UNIQUE_IDENTIFIER_0"/>
0163	<Attribute>
0164	<AttributeName type="TextString" value="x-provider"/>
0165	<AttributeValue type="TextString" value="unknown"/>
0166	</Attribute>
0167	</RequestPayload>
0168	</BatchItem>
0169	</RequestMessage>
0170	# [Client-to-Server]
0171	<ResponseMessage>
0172	<ResponseHeader>
0173	<ProtocolVersion>
0174	<ProtocolVersionMajor type="Integer" value="1"/>

0170	<ProtocolVersionMinor type="Integer" value="2"/>
0171	</ProtocolVersion>
0172	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0173	<BatchCount type="Integer" value="1"/>
0174	</ResponseHeader>
0175	<BatchItem>
0176	<Operation type="Enumeration" value="AddAttribute"/>
0177	<ResultStatus type="Enumeration" value="Success"/>
0178	<ResponsePayload>
0179	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0180	<Attribute>
0181	<AttributeName type="TextString" value="x-provider"/>
0182	<AttributeValue type="TextString" value="unknown"/>
0183	</Attribute>
0184	</ResponsePayload>
0185	</BatchItem>
0186	</ResponseMessage>
	# TIME 3
	# [Server-to-Client]
0187	<RequestMessage>
0188	<RequestHeader>
0189	<ProtocolVersion>
0190	<ProtocolVersionMajor type="Integer" value="1"/>
0191	<ProtocolVersionMinor type="Integer" value="0"/>
0192	</ProtocolVersion>
0193	<BatchCount type="Integer" value="1"/>
0194	</RequestHeader>
0195	<BatchItem>
0196	<Operation type="Enumeration" value="Notify"/>
0197	<RequestPayload>
0198	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0199	<Attribute>
0200	<AttributeName type="TextString" value="x-provider"/>
0201	<AttributeValue type="TextString" value="unknown"/>
0202	</Attribute>
0203	<Attribute>
0204	<AttributeName type="TextString" value="Last Change Date"/>
0205	<AttributeValue type="DateTime" value="2013-06-
	26T05:54:18+00:00"/>
0206	</Attribute>
0207	</RequestPayload>
0208	</BatchItem>
0209	</RequestMessage>
	# [Server-to-Client]
0210	<ResponseMessage>
0211	<ResponseHeader>
0212	<ProtocolVersion>
0213	<ProtocolVersionMajor type="Integer" value="1"/>
0214	<ProtocolVersionMinor type="Integer" value="0"/>
0215	</ProtocolVersion>
0216	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0217	<BatchCount type="Integer" value="1"/>
0218	</ResponseHeader>
0219	<BatchItem>
0220	<Operation type="Enumeration" value="Notify"/>

0221	<ResultStatus type="Enumeration" value="Success"/>
0222	<ResponsePayload>
0223	</ResponsePayload>
0224	</BatchItem>
0225	</ResponseMessage>
# TIME 4 # [Client-to-Server]	
0226	<RequestMessage>
0227	<RequestHeader>
0228	<ProtocolVersion>
0229	<ProtocolVersionMajor type="Integer" value="1"/>
0230	<ProtocolVersionMinor type="Integer" value="2"/>
0231	</ProtocolVersion>
0232	<BatchCount type="Integer" value="1"/>
0233	</RequestHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="ModifyAttribute"/>
0236	<RequestPayload>
0237	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0238	<Attribute>
0239	<AttributeName type="TextString" value="x-provider"/>
0240	<AttributeValue type="TextString" value="third party"/>
0241	</Attribute>
0242	</RequestPayload>
0243	</BatchItem>
0244	</RequestMessage>
# [Client-to-Server]	
0245	<ResponseMessage>
0246	<ResponseHeader>
0247	<ProtocolVersion>
0248	<ProtocolVersionMajor type="Integer" value="1"/>
0249	<ProtocolVersionMinor type="Integer" value="2"/>
0250	</ProtocolVersion>
0251	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0252	<BatchCount type="Integer" value="1"/>
0253	</ResponseHeader>
0254	<BatchItem>
0255	<Operation type="Enumeration" value="ModifyAttribute"/>
0256	<ResultStatus type="Enumeration" value="Success"/>
0257	<ResponsePayload>
0258	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0259	<Attribute>
0260	<AttributeName type="TextString" value="x-provider"/>
0261	<AttributeValue type="TextString" value="third party"/>
0262	</Attribute>
0263	</ResponsePayload>
0264	</BatchItem>
0265	</ResponseMessage>
# TIME 5 # [Server-to-Client]	
0266	<RequestMessage>
0267	<RequestHeader>
0268	<ProtocolVersion>
0269	<ProtocolVersionMajor type="Integer" value="1"/>

0270	<ProtocolVersionMinor type="Integer" value="0"/>
0271	</ProtocolVersion>
0272	<BatchCount type="Integer" value="1"/>
0273	</RequestHeader>
0274	<BatchItem>
0275	<Operation type="Enumeration" value="Notify"/>
0276	<RequestPayload>
0277	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0278	<Attribute>
0279	<AttributeName type="TextString" value="x-provider"/>
0280	<AttributeValue type="TextString" value="third party"/>
0281	</Attribute>
0282	<Attribute>
0283	<AttributeName type="TextString" value="Last Change Date"/>
0284	<AttributeValue type="DateTime" value="2013-06- 26T05:54:18+00:00"/>
0285	</Attribute>
0286	</RequestPayload>
0287	</BatchItem>
0288	</RequestMessage>
# [Server-to-Client]	
0289	<ResponseMessage>
0290	<ResponseHeader>
0291	<ProtocolVersion>
0292	<ProtocolVersionMajor type="Integer" value="1"/>
0293	<ProtocolVersionMinor type="Integer" value="0"/>
0294	</ProtocolVersion>
0295	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0296	<BatchCount type="Integer" value="1"/>
0297	</ResponseHeader>
0298	<BatchItem>
0299	<Operation type="Enumeration" value="Notify"/>
0300	<ResultStatus type="Enumeration" value="Success"/>
0301	<ResponsePayload>
0302	</ResponsePayload>
0303	</BatchItem>
0304	</ResponseMessage>
# TIME 6	
# [Client-to-Server]	
0305	<RequestMessage>
0306	<RequestHeader>
0307	<ProtocolVersion>
0308	<ProtocolVersionMajor type="Integer" value="1"/>
0309	<ProtocolVersionMinor type="Integer" value="2"/>
0310	</ProtocolVersion>
0311	<BatchCount type="Integer" value="1"/>
0312	</RequestHeader>
0313	<BatchItem>
0314	<Operation type="Enumeration" value="Destroy"/>
0315	<RequestPayload>
0316	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0317	</RequestPayload>
0318	</BatchItem>
0319	</RequestMessage>

0320	# [Client-to-Server]
0321	<ResponseMessage>
0322	<ResponseHeader>
0323	<ProtocolVersion>
0324	<ProtocolVersionMajor type="Integer" value="1"/>
0325	<ProtocolVersionMinor type="Integer" value="2"/>
0326	</ProtocolVersion>
0327	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0328	<BatchCount type="Integer" value="1"/>
0329	</ResponseHeader>
0330	<BatchItem>
0331	<Operation type="Enumeration" value="Destroy"/>
0332	<ResultStatus type="Enumeration" value="Success"/>
0333	<ResponsePayload>
0334	<UniqueIdentifier type="TextString"
0335	value="\$UNIQUE_IDENTIFIER_0"/>
0336	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>
	# TIME 7
	# [Server-to-Client]
0337	<RequestMessage>
0338	<RequestHeader>
0339	<ProtocolVersion>
0340	<ProtocolVersionMajor type="Integer" value="1"/>
0341	<ProtocolVersionMinor type="Integer" value="0"/>
0342	</ProtocolVersion>
0343	<BatchCount type="Integer" value="1"/>
0344	</RequestHeader>
0345	<BatchItem>
0346	<Operation type="Enumeration" value="Notify"/>
0347	<RequestPayload>
0348	<UniqueIdentifier type="TextString"
0349	value="\$UNIQUE_IDENTIFIER_0"/>
0350	<Attribute>
0351	<AttributeName type="TextString" value="Last Change Date"/>
0352	<AttributeValue type="DateTime" value="2013-06-
0353	26T05:54:18+00:00"/>
0354	</Attribute>
0355	<Attribute>
0356	<AttributeName type="TextString" value="State"/>
0357	<AttributeValue type="Enumeration" value="Destroyed"/>
0358	</Attribute>
0359	</RequestPayload>
	</BatchItem>
	</RequestMessage>
0360	# [Server-to-Client]
0361	<ResponseMessage>
0362	<ResponseHeader>
0363	<ProtocolVersion>
0364	<ProtocolVersionMajor type="Integer" value="1"/>
0365	<ProtocolVersionMinor type="Integer" value="0"/>
0366	</ProtocolVersion>
0367	<TimeStamp type="DateTime" value="2013-06-26T05:54:18+00:00"/>
0368	<BatchCount type="Integer" value="1"/>
0369	</ResponseHeader>
	<BatchItem>

0370	<Operation type="Enumeration" value="Notify"/>
0371	<ResultStatus type="Enumeration" value="Success"/>
0372	<ResponsePayload>
0373	</ResponsePayload>
0374	</BatchItem>
0375	</ResponseMessage>

1059

1060 2.3.39 TC-ECC-1-12 - Register an ECC Key Pair

1061 EC recommended curve is secp256k1

1062 - Private Key format ECPrivateKey - <http://tools.ietf.org/html/rfc5915>

1063 - Public Key format SubjectPublicKeyInfo - <http://tools.ietf.org/html/rfc5480>

1064 Register a EC private key in the ECPrivateKey key format, then register the corresponding public
1065 key, in X.509 (SubjectPublicKeyInfo) format, with the Link attribute pointing to the previously
1066 registered private key. Then add the Link attribute to the private key, and perform Locate
1067 operations to find the public and private keys using the Link attribute. Get both the private and
1068 public keys in default format, then destroy both the private and the public key.

1069

1070 -----BEGIN EC PRIVATE KEY-----
1071 MHQCAQEEINTNeowwyjCeYsQB11jAC6JE3WTZv1KjEHIGa4oAwZxooAcGBSuBBAK
1072 oUQDQgAE2rXTwLMRPbQUq/wcDr9aAlWeZWqhyLCqjYcKoDJM2kiZkl6h5tvCWabH
1073 glz0ZZKsdZTMQL1gS3KNiLY28xfTZg==
1074 -----END EC PRIVATE KEY-----
1075
1076 -----BEGIN PUBLIC KEY-----
1077 MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAE2rXTwLMRPbQUq/wcDr9aAlWeZWqhyLCq
1078 jYcKoDJM2kiZkl6h5tvCWabHglz0ZZKsdZTMQL1gS3KNiLY28xfTZg==
1079 -----END PUBLIC KEY-----
1080
1081

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="PrivateKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Sign"/>

0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-ECC-1-12- prikey1"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<PrivateKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="ECPrivateKey"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString" value="30740201010420db4d128c30ca309e62c4019758c00ba244dd64d9bf52a31 078866b8a00c19c68a00706052b8104000aa14403420004dab5d3c253113db414abf c1c0ebf5a02559e656aa1c8b0aa8d870aa0324cda4899925eale6dbc259a6c7825cf 46592ac7594cc40bd604b728d88b636f317d366"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="EC"/>
0030	<CryptographicLength type="Integer" value="256"/>
0031	</KeyBlock>
0032	</PrivateKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="2"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="2"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PublicKey"/>
0065	<TemplateAttribute>
0066	<Attribute>

0067	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0068	<AttributeValue type="Integer" value="Verify"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>
0073	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0075	</AttributeValue>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-ECC-1-12-pubkey1"/>
0080	</Attribute>
0081	</TemplateAttribute>
0082	<PublicKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="X_509"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString" value="3056301006072a8648ce3d020106052b8104000a03420004dab5d3c253113db414abfc1c0ebf5a02559e656aa1c8b0aa8d870aa0324cda4899925eale6dbc259a6c7825cf46592ac7594cc40bd604b728d88b636f317d366"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="EC"/>
0089	<CryptographicLength type="Integer" value="256"/>
0090	</KeyBlock>
0091	</PublicKey>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="2"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0109	</ResponsePayload>
0110	</BatchItem>
0111	</ResponseMessage>
	# TIME 2
0112	<RequestMessage>
0113	<RequestHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>

0116	<ProtocolVersionMinor type="Integer" value="2"/>
0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="AddAttribute"/>
0122	<RequestPayload>
0123	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Link"/>
0126	<AttributeValue>
0127	<LinkType type="Enumeration" value="PublicKeyLink"/>
0128	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0129	</AttributeValue>
0130	</Attribute>
0131	</RequestPayload>
0132	</BatchItem>
0133	</RequestMessage>
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="2"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="AddAttribute"/>
0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0148	<Attribute>
0149	<AttributeName type="TextString" value="Link"/>
0150	<AttributeValue>
0151	<LinkType type="Enumeration" value="PublicKeyLink"/>
0152	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0153	</AttributeValue>
0154	</Attribute>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
	# TIME 3
0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="2"/>
0163	</ProtocolVersion>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Locate"/>

0168	<RequestPayload>
0169	<Attribute>
0170	<AttributeName type="TextString" value="Object Type"/>
0171	<AttributeValue type="Enumeration" value="PublicKey"/>
0172	</Attribute>
0173	<Attribute>
0174	<AttributeName type="TextString" value="Link"/>
0175	<AttributeValue>
0176	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0177	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0178	</AttributeValue>
0179	</Attribute>
0180	</RequestPayload>
0181	</BatchItem>
0182	</RequestMessage>
0183	<ResponseMessage>
0184	<ResponseHeader>
0185	<ProtocolVersion>
0186	<ProtocolVersionMajor type="Integer" value="1"/>
0187	<ProtocolVersionMinor type="Integer" value="2"/>
0188	</ProtocolVersion>
0189	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0190	<BatchCount type="Integer" value="1"/>
0191	</ResponseHeader>
0192	<BatchItem>
0193	<Operation type="Enumeration" value="Locate"/>
0194	<ResultStatus type="Enumeration" value="Success"/>
0195	<ResponsePayload>
0196	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0197	</ResponsePayload>
0198	</BatchItem>
0199	</ResponseMessage>
	# TIME 4
0200	<RequestMessage>
0201	<RequestHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="2"/>
0205	</ProtocolVersion>
0206	<BatchCount type="Integer" value="1"/>
0207	</RequestHeader>
0208	<BatchItem>
0209	<Operation type="Enumeration" value="Locate"/>
0210	<RequestPayload>
0211	<Attribute>
0212	<AttributeName type="TextString" value="Object Type"/>
0213	<AttributeValue type="Enumeration" value="PrivateKey"/>
0214	</Attribute>
0215	<Attribute>
0216	<AttributeName type="TextString" value="Link"/>
0217	<AttributeValue>
0218	<LinkType type="Enumeration" value="PublicKeyLink"/>
0219	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0220	</AttributeValue>

0221	</Attribute>
0222	</RequestPayload>
0223	</BatchItem>
0224	</RequestMessage>
0225	<ResponseMessage>
0226	<ResponseHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="2"/>
0230	</ProtocolVersion>
0231	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0232	<BatchCount type="Integer" value="1"/>
0233	</ResponseHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="Locate"/>
0236	<ResultStatus type="Enumeration" value="Success"/>
0237	<ResponsePayload>
0238	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0239	</ResponsePayload>
0240	</BatchItem>
0241	</ResponseMessage>
# TIME 5	
0242	<RequestMessage>
0243	<RequestHeader>
0244	<ProtocolVersion>
0245	<ProtocolVersionMajor type="Integer" value="1"/>
0246	<ProtocolVersionMinor type="Integer" value="2"/>
0247	</ProtocolVersion>
0248	<BatchCount type="Integer" value="1"/>
0249	</RequestHeader>
0250	<BatchItem>
0251	<Operation type="Enumeration" value="Get"/>
0252	<RequestPayload>
0253	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0254	</RequestPayload>
0255	</BatchItem>
0256	</RequestMessage>
0257	<ResponseMessage>
0258	<ResponseHeader>
0259	<ProtocolVersion>
0260	<ProtocolVersionMajor type="Integer" value="1"/>
0261	<ProtocolVersionMinor type="Integer" value="2"/>
0262	</ProtocolVersion>
0263	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0264	<BatchCount type="Integer" value="1"/>
0265	</ResponseHeader>
0266	<BatchItem>
0267	<Operation type="Enumeration" value="Get"/>
0268	<ResultStatus type="Enumeration" value="Success"/>
0269	<ResponsePayload>
0270	<ObjectType type="Enumeration" value="PrivateKey"/>
0271	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0272	<PrivateKey>

0273	<KeyBlock>
0274	<KeyFormatType type="Enumeration" value="ECPrivateKey"/>
0275	<KeyValue>
0276	<KeyMaterial type="ByteString"
	value="30740201010420db4d128c30ca309e62c4019758c00ba244dd64d9bf52a31
	078866b8a00c19c68a00706052b8104000aa14403420004dab5d3c253113db414abf
	c1c0ebf5a02559e656aa1c8b0aa8d870aa0324cda4899925ea1e6dbc259a6c7825cf
	46592ac7594cc40bd604b728d88b636f317d366"/>
0277	</KeyValue>
0278	<CryptographicAlgorithm type="Enumeration" value="EC"/>
0279	<CryptographicLength type="Integer" value="256"/>
0280	</KeyBlock>
0281	</PrivateKey>
0282	</ResponsePayload>
0283	</BatchItem>
0284	</ResponseMessage>
	# TIME 6
0285	<RequestMessage>
0286	<RequestHeader>
0287	<ProtocolVersion>
0288	<ProtocolVersionMajor type="Integer" value="1"/>
0289	<ProtocolVersionMinor type="Integer" value="2"/>
0290	</ProtocolVersion>
0291	<BatchCount type="Integer" value="1"/>
0292	</RequestHeader>
0293	<BatchItem>
0294	<Operation type="Enumeration" value="Get"/>
0295	<RequestPayload>
0296	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0297	</RequestPayload>
0298	</BatchItem>
0299	</RequestMessage>
0300	<ResponseMessage>
0301	<ResponseHeader>
0302	<ProtocolVersion>
0303	<ProtocolVersionMajor type="Integer" value="1"/>
0304	<ProtocolVersionMinor type="Integer" value="2"/>
0305	</ProtocolVersion>
0306	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0307	<BatchCount type="Integer" value="1"/>
0308	</ResponseHeader>
0309	<BatchItem>
0310	<Operation type="Enumeration" value="Get"/>
0311	<ResultStatus type="Enumeration" value="Success"/>
0312	<ResponsePayload>
0313	<ObjectType type="Enumeration" value="PublicKey"/>
0314	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0315	<PublicKey>
0316	<KeyBlock>
0317	<KeyFormatType type="Enumeration" value="X_509"/>
0318	<KeyValue>
0319	<KeyMaterial type="ByteString"
	value="3056301006072a8648ce3d020106052b8104000a03420004dab5d3c253113
	db414abfc1c0ebf5a02559e656aa1c8b0aa8d870aa0324cda4899925ea1e6dbc259a
	6c7825cf46592ac7594cc40bd604b728d88b636f317d366"/>

0320	</KeyValue>
0321	<CryptographicAlgorithm type="Enumeration" value="EC"/>
0322	<CryptographicLength type="Integer" value="256"/>
0323	</KeyBlock>
0324	</PublicKey>
0325	</ResponsePayload>
0326	</BatchItem>
0327	</ResponseMessage>
# TIME 7	
0328	<RequestMessage>
0329	<RequestHeader>
0330	<ProtocolVersion>
0331	<ProtocolVersionMajor type="Integer" value="1"/>
0332	<ProtocolVersionMinor type="Integer" value="2"/>
0333	</ProtocolVersion>
0334	<BatchCount type="Integer" value="1"/>
0335	</RequestHeader>
0336	<BatchItem>
0337	<Operation type="Enumeration" value="Destroy"/>
0338	<RequestPayload>
0339	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0340	</RequestPayload>
0341	</BatchItem>
0342	</RequestMessage>
0343	<ResponseMessage>
0344	<ResponseHeader>
0345	<ProtocolVersion>
0346	<ProtocolVersionMajor type="Integer" value="1"/>
0347	<ProtocolVersionMinor type="Integer" value="2"/>
0348	</ProtocolVersion>
0349	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0350	<BatchCount type="Integer" value="1"/>
0351	</ResponseHeader>
0352	<BatchItem>
0353	<Operation type="Enumeration" value="Destroy"/>
0354	<ResultStatus type="Enumeration" value="Success"/>
0355	<ResponsePayload>
0356	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0357	</ResponsePayload>
0358	</BatchItem>
0359	</ResponseMessage>
# TIME 8	
0360	<RequestMessage>
0361	<RequestHeader>
0362	<ProtocolVersion>
0363	<ProtocolVersionMajor type="Integer" value="1"/>
0364	<ProtocolVersionMinor type="Integer" value="2"/>
0365	</ProtocolVersion>
0366	<BatchCount type="Integer" value="1"/>
0367	</RequestHeader>
0368	<BatchItem>
0369	<Operation type="Enumeration" value="Destroy"/>
0370	<RequestPayload>
0371	<UniqueIdentifier type="TextString"

0372	value="\$UNIQUE_IDENTIFIER_1"/>
0373	</RequestPayload>
0374	</BatchItem>
0375	</RequestMessage>
0375	<ResponseMessage>
0376	<ResponseHeader>
0377	<ProtocolVersion>
0378	<ProtocolVersionMajor type="Integer" value="1"/>
0379	<ProtocolVersionMinor type="Integer" value="2"/>
0380	</ProtocolVersion>
0381	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0382	<BatchCount type="Integer" value="1"/>
0383	</ResponseHeader>
0384	<BatchItem>
0385	<Operation type="Enumeration" value="Destroy"/>
0386	<ResultStatus type="Enumeration" value="Success"/>
0387	<ResponsePayload>
0388	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0389	</ResponsePayload>
0390	</BatchItem>
0391	</ResponseMessage>

1082

1083 2.3.40 TC-ECC-2-12 - Register an ECC Key Pair in PKCS8 Format

1084 EC recommended curve is secp256k1

1085 - Public Key format SubjectPublicKeyInfo - <http://tools.ietf.org/html/rfc5480>

1086 Register a EC private key in PKCS8 key format (with passphrase 'secret' using pbeWithSHAAnd3-
1087 KeyTripleDES-CBC), then register the corresponding public key, in X.509 (SubjectPublicKeyInfo)
1088 format, with the Link attribute pointing to the previously registered private key. Then add the
1089 Link attribute to the private key, and perform Locate operations to find the public and private
1090 keys using the Link attribute. Get both the private and public keys in default format, then
1091 destroy both the private and the public key.

1092

1093 -----BEGIN ENCRYPTED PRIVATE KEY-----
1094 MIGpMBwGCIqGSib3DQEMAQMwDgQIrlU0TS8GObcCAggABIGIA7njjI0W9Cmq6ORn
1095 eFHqc9yko1oSsvg8aETKc4sZxLOAHG2u5RcHqOIWvXLTQmzU8m3yZhlZDz1OIJfg
1096 w2X8XZ2gPAo8CAkbuZRO2lwzey2ZZnigF2u3z6PtX+fyyn6jOou17SeaYp0OUx0
1097 ovFD2eJEWlcOa9TkBeVhK4ziaHHuv0jH5Wxt4A==
1098 -----END ENCRYPTED PRIVATE KEY-----
1099
1100 -----BEGIN PUBLIC KEY-----
1101 MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAE2rXTwlMRPbQUq/wcDr9aAlWeZWqhyLCq
1102 jYcKoDJM2kiZkl6h5tvCWabHglz0ZZKsdZTMQL1gS3KNiLY28xfTZg==
1103 -----END PUBLIC KEY-----
1104

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>

0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="PrivateKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Sign"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-ECC-2-12- prikey1"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<PrivateKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="PKCS_8"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString" value="3081a9301c060a2a864886f70d010c0103300e0408dc4dc656aa7bcc04020 20800048188824b0a6786064a1d5686b852d8ff3073cb3379397dee978c60031353e 1835a1a3c6289f16ff617b2d8b2d32829c265b997b406a69b96894caa39ceelc556c da380e7174271606a4dfde4bc6182943de6e827573ce3d877b72f1cdd3a59a3721b3 4740466fa43390ab29fb8ac01df172f9af6bb222aeee0f9be744b425e9620902ebc7 6ab8ceaa555"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="EC"/>
0030	<CryptographicLength type="Integer" value="256"/>
0031	</KeyBlock>
0032	</PrivateKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="2"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>

0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="2"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PublicKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0068	<AttributeValue type="Integer" value="Verify"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>
0073	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0075	</AttributeValue>
0076	</Attribute>
0077	<Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-ECC-2-12-pubkey1"/>
0080	</Attribute>
0081	</TemplateAttribute>
0082	<PublicKey>
0083	<KeyBlock>
0084	<KeyFormatType type="Enumeration" value="X_509"/>
0085	<KeyValue>
0086	<KeyMaterial type="ByteString" value="3056301006072a8648ce3d020106052b8104000a03420004dab5d3c253113db414abfc1c0ebf5a02559e656aa1c8b0aa8d870aa0324cda4899925eale6dbc259a6c7825cf46592ac7594cc40bd604b728d88b636f317d366"/>
0087	</KeyValue>
0088	<CryptographicAlgorithm type="Enumeration" value="EC"/>
0089	<CryptographicLength type="Integer" value="256"/>
0090	</KeyBlock>
0091	</PublicKey>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="2"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>

0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="Register"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0109	</ResponsePayload>
0110	</BatchItem>
0111	</ResponseMessage>
# TIME 2	
0112	<RequestMessage>
0113	<RequestHeader>
0114	<ProtocolVersion>
0115	<ProtocolVersionMajor type="Integer" value="1"/>
0116	<ProtocolVersionMinor type="Integer" value="2"/>
0117	</ProtocolVersion>
0118	<BatchCount type="Integer" value="1"/>
0119	</RequestHeader>
0120	<BatchItem>
0121	<Operation type="Enumeration" value="AddAttribute"/>
0122	<RequestPayload>
0123	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Link"/>
0126	<AttributeValue>
0127	<LinkType type="Enumeration" value="PublicKeyLink"/>
0128	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0129	</AttributeValue>
0130	</Attribute>
0131	</RequestPayload>
0132	</BatchItem>
0133	</RequestMessage>
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="2"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="AddAttribute"/>
0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0148	<Attribute>
0149	<AttributeName type="TextString" value="Link"/>
0150	<AttributeValue>
0151	<LinkType type="Enumeration" value="PublicKeyLink"/>
0152	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>

0153	</AttributeValue>
0154	</Attribute>
0155	</ResponsePayload>
0156	</BatchItem>
0157	</ResponseMessage>
0158	# TIME 3
0158	<RequestMessage>
0159	<RequestHeader>
0160	<ProtocolVersion>
0161	<ProtocolVersionMajor type="Integer" value="1"/>
0162	<ProtocolVersionMinor type="Integer" value="2"/>
0163	</ProtocolVersion>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Locate"/>
0168	<RequestPayload>
0169	<Attribute>
0170	<AttributeName type="TextString" value="Object Type"/>
0171	<AttributeValue type="Enumeration" value="PublicKey"/>
0172	</Attribute>
0173	<Attribute>
0174	<AttributeName type="TextString" value="Link"/>
0175	<AttributeValue>
0176	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0177	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0178	</AttributeValue>
0179	</Attribute>
0180	</RequestPayload>
0181	</BatchItem>
0182	</RequestMessage>
0183	<ResponseMessage>
0184	<ResponseHeader>
0185	<ProtocolVersion>
0186	<ProtocolVersionMajor type="Integer" value="1"/>
0187	<ProtocolVersionMinor type="Integer" value="2"/>
0188	</ProtocolVersion>
0189	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0190	<BatchCount type="Integer" value="1"/>
0191	</ResponseHeader>
0192	<BatchItem>
0193	<Operation type="Enumeration" value="Locate"/>
0194	<ResultStatus type="Enumeration" value="Success"/>
0195	<ResponsePayload>
0196	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0197	</ResponsePayload>
0198	</BatchItem>
0199	</ResponseMessage>
	# TIME 4
0200	<RequestMessage>
0201	<RequestHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="2"/>

0205	</ProtocolVersion>
0206	<BatchCount type="Integer" value="1"/>
0207	</RequestHeader>
0208	<BatchItem>
0209	<Operation type="Enumeration" value="Locate"/>
0210	<RequestPayload>
0211	<Attribute>
0212	<AttributeName type="TextString" value="Object Type"/>
0213	<AttributeValue type="Enumeration" value="PrivateKey"/>
0214	</Attribute>
0215	<Attribute>
0216	<AttributeName type="TextString" value="Link"/>
0217	<AttributeValue>
0218	<LinkType type="Enumeration" value="PublicKeyLink"/>
0219	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0220	</AttributeValue>
0221	</Attribute>
0222	</RequestPayload>
0223	</BatchItem>
0224	</RequestMessage>
0225	<ResponseMessage>
0226	<ResponseHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="2"/>
0230	</ProtocolVersion>
0231	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0232	<BatchCount type="Integer" value="1"/>
0233	</ResponseHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="Locate"/>
0236	<ResultStatus type="Enumeration" value="Success"/>
0237	<ResponsePayload>
0238	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0239	</ResponsePayload>
0240	</BatchItem>
0241	</ResponseMessage>
	# TIME 5
0242	<RequestMessage>
0243	<RequestHeader>
0244	<ProtocolVersion>
0245	<ProtocolVersionMajor type="Integer" value="1"/>
0246	<ProtocolVersionMinor type="Integer" value="2"/>
0247	</ProtocolVersion>
0248	<BatchCount type="Integer" value="1"/>
0249	</RequestHeader>
0250	<BatchItem>
0251	<Operation type="Enumeration" value="Get"/>
0252	<RequestPayload>
0253	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0254	</RequestPayload>
0255	</BatchItem>
0256	</RequestMessage>

0257	<ResponseMessage>
0258	<ResponseHeader>
0259	<ProtocolVersion>
0260	<ProtocolVersionMajor type="Integer" value="1"/>
0261	<ProtocolVersionMinor type="Integer" value="2"/>
0262	</ProtocolVersion>
0263	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0264	<BatchCount type="Integer" value="1"/>
0265	</ResponseHeader>
0266	<BatchItem>
0267	<Operation type="Enumeration" value="Get"/>
0268	<ResultStatus type="Enumeration" value="Success"/>
0269	<ResponsePayload>
0270	<ObjectType type="Enumeration" value="PrivateKey"/>
0271	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0272	<PrivateKey>
0273	<KeyBlock>
0274	<KeyFormatType type="Enumeration" value="PKCS_8"/>
0275	<KeyValue>
0276	<KeyMaterial type="ByteString"
	value="30740201010420db4d128c30ca309e62c4019758c00ba244dd64d9bf52a31078866b8a00c19c68a00706052b8104000aa14403420004dab5d3c253113db414abfc1c0ebf5a02559e656aa1c8b0aa8d870aa0324cda4899925ea1e6dbc259a6c7825cf46592ac7594cc40bd604b728d88b636f317d366"/>
0277	</KeyValue>
0278	<CryptographicAlgorithm type="Enumeration" value="EC"/>
0279	<CryptographicLength type="Integer" value="256"/>
0280	</KeyBlock>
0281	</PrivateKey>
0282	</ResponsePayload>
0283	</BatchItem>
0284	</ResponseMessage>
	# TIME 6
0285	<RequestMessage>
0286	<RequestHeader>
0287	<ProtocolVersion>
0288	<ProtocolVersionMajor type="Integer" value="1"/>
0289	<ProtocolVersionMinor type="Integer" value="2"/>
0290	</ProtocolVersion>
0291	<BatchCount type="Integer" value="1"/>
0292	</RequestHeader>
0293	<BatchItem>
0294	<Operation type="Enumeration" value="Get"/>
0295	<RequestPayload>
0296	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0297	</RequestPayload>
0298	</BatchItem>
0299	</RequestMessage>
0300	<ResponseMessage>
0301	<ResponseHeader>
0302	<ProtocolVersion>
0303	<ProtocolVersionMajor type="Integer" value="1"/>
0304	<ProtocolVersionMinor type="Integer" value="2"/>
0305	</ProtocolVersion>
0306	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>

0307	<BatchCount type="Integer" value="1"/>
0308	</ResponseHeader>
0309	<BatchItem>
0310	<Operation type="Enumeration" value="Get"/>
0311	<ResultStatus type="Enumeration" value="Success"/>
0312	<ResponsePayload>
0313	<ObjectType type="Enumeration" value="PublicKey"/>
0314	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0315	<PublicKey>
0316	<KeyBlock>
0317	<KeyFormatType type="Enumeration" value="X_509"/>
0318	<KeyValue>
0319	<KeyMaterial type="ByteString"
	value="3056301006072a8648ce3d020106052b8104000a03420004dab5d3c253113
	db414abfc1c0ebf5a02559e656aa1c8b0aa8d870aa0324cda4899925eale6dbc259a
	6c7825cf46592ac7594cc40bd604b728d88b636f317d366"/>
0320	</KeyValue>
0321	<CryptographicAlgorithm type="Enumeration" value="EC"/>
0322	<CryptographicLength type="Integer" value="256"/>
0323	</KeyBlock>
0324	</PublicKey>
0325	</ResponsePayload>
0326	</BatchItem>
0327	</ResponseMessage>
	# TIME 7
0328	<RequestMessage>
0329	<RequestHeader>
0330	<ProtocolVersion>
0331	<ProtocolVersionMajor type="Integer" value="1"/>
0332	<ProtocolVersionMinor type="Integer" value="2"/>
0333	</ProtocolVersion>
0334	<BatchCount type="Integer" value="1"/>
0335	</RequestHeader>
0336	<BatchItem>
0337	<Operation type="Enumeration" value="Destroy"/>
0338	<RequestPayload>
0339	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0340	</RequestPayload>
0341	</BatchItem>
0342	</RequestMessage>
0343	<ResponseMessage>
0344	<ResponseHeader>
0345	<ProtocolVersion>
0346	<ProtocolVersionMajor type="Integer" value="1"/>
0347	<ProtocolVersionMinor type="Integer" value="2"/>
0348	</ProtocolVersion>
0349	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0350	<BatchCount type="Integer" value="1"/>
0351	</ResponseHeader>
0352	<BatchItem>
0353	<Operation type="Enumeration" value="Destroy"/>
0354	<ResultStatus type="Enumeration" value="Success"/>
0355	<ResponsePayload>
0356	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0357	</ResponsePayload>
0358	</BatchItem>
0359	</ResponseMessage>
# TIME 8	
0360	<RequestMessage>
0361	<RequestHeader>
0362	<ProtocolVersion>
0363	<ProtocolVersionMajor type="Integer" value="1"/>
0364	<ProtocolVersionMinor type="Integer" value="2"/>
0365	</ProtocolVersion>
0366	<BatchCount type="Integer" value="1"/>
0367	</RequestHeader>
0368	<BatchItem>
0369	<Operation type="Enumeration" value="Destroy"/>
0370	<RequestPayload>
0371	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0372	</RequestPayload>
0373	</BatchItem>
0374	</RequestMessage>
0375	<ResponseMessage>
0376	<ResponseHeader>
0377	<ProtocolVersion>
0378	<ProtocolVersionMajor type="Integer" value="1"/>
0379	<ProtocolVersionMinor type="Integer" value="2"/>
0380	</ProtocolVersion>
0381	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0382	<BatchCount type="Integer" value="1"/>
0383	</ResponseHeader>
0384	<BatchItem>
0385	<Operation type="Enumeration" value="Destroy"/>
0386	<ResultStatus type="Enumeration" value="Success"/>
0387	<ResponsePayload>
0388	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0389	</ResponsePayload>
0390	</BatchItem>
0391	</ResponseMessage>

1105

1106 2.3.41 TC-ECC-3-12 - Register an ECC Key Pair and ECDSA Certificate

1107 EC recommended curve is secp256k1

1108 - Private Key format ECPrivateKey - <http://tools.ietf.org/html/rfc5915>

1109 - Public Key format SubjectPublicKeyInfo - <http://tools.ietf.org/html/rfc5480>

1110 Register a EC private key in the ECPrivateKey key format, then register the corresponding public
1111 key, in X.509 (SubjectPublicKeyInfo) format, and a corresponding ECDSA certificate, with the
1112 Link attribute pointing to the previously registered private key. Return the attribute values for
1113 the ECDSA certificate showing the correct server parsing of the certificate. Then add the Link
1114 attribute to the private key, and perform Locate operations to find the public and private keys

1115 using the Link attribute. Get both the private and public keys in default format, then destroy
1116 both the private and the public key.

1117

```

1118 -----BEGIN EC PRIVATE KEY-----
1119 MHQCAQEEINTNEowwyjCeYsQB11jAC6JE3WTZv1KjEHIGa4oAwZxooAcGBSuBBAK
1120 oUQDQgAE2rXTwLMRPbQUq/wcDr9aAlWeZWqhyLCqjYcKoDJM2kiZkl6h5tvCWabH
1121 glz0ZZKsdZTMQL1gS3KNiLY28xfTZg==
1122 -----END EC PRIVATE KEY-----
1123
1124 -----BEGIN PUBLIC KEY-----
1125 MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAE2rXTwLMRPbQUq/wcDr9aAlWeZWqhyLCq
1126 jYcKoDJM2kiZkl6h5tvCWabHglz0ZZKsdZTMQL1gS3KNiLY28xfTZg==
1127 -----END PUBLIC KEY-----
1128
1129 -----BEGIN CERTIFICATE-----
1130 MIIB1TCCAXqgAwIBAgIJAOWLdAIzVbKVMAoGCCqGSM49BAMCEGxCzAJBgNVBAYT
1131 AlVTMQ0wCwYDVQQKDARURVNUMQ4wDAYDVQQQLDAVPQVNUzEaMBGGA1UEAwRS01J
1132 UC1FQY1zZWNwMjU2azEwHhcNMjMwNjI1MTAzMzExWhcNMjMwNjI1MTAzMzExWjBI
1133 MQswCQYDVQQGEwJVUzENMAAsGA1UECgwEVEVTVDEOMAwGA1UECwwFT0FTSVMxGjAY
1134 BgNVBAMMEUtNSVAtRUMtc2VjcDI1NmsxMFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAE
1135 2rXTwLMRPbQUq/wcDr9aAlWeZWqhyLCqjYcKoDJM2kiZkl6h5tvCWabHglz0ZZKs
1136 dZTMQL1gS3KNiLY28xfTZgNQME4wHQYDVRO0BBYEFKCY1LuogX9+lQaMh1++yFCz
1137 4XegMB8GA1UdIwQYMBaAFKCY1LuogX9+lQaMh1++yFCz4XegMAwGA1UdEwQFMAMB
1138 Af8wCgYIKoZIzj0EAwIDSQAwRgIhAOnNFLY+PlfdJt37p3o+0dBbNyFFT2F1Cd/z
1139 ua8C1PWuAiEAYa/vk0S4+LEsUltGGNw2Ibzn+LOQrAH/vmhsx2Qcdrs=
1140 -----END CERTIFICATE-----
1141
1142
```

#	TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="PrivateKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Sign"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-ECC-3-12-prikey1"/>
0021	</Attribute>
0022	</TemplateAttribute>

0023	<PrivateKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="ECPrivateKey"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString"
	value="30740201010420db4d128c30ca309e62c4019758c00ba244dd64d9bf52a31
	078866b8a00c19c68a00706052b8104000aa14403420004dab5d3c253113db414abf
	c1c0ebf5a02559e656aa1c8b0aa8d870aa0324cda4899925eale6dbc259a6c7825cf
	46592ac7594cc40bd604b728d88b636f317d366"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="EC"/>
0030	<CryptographicLength type="Integer" value="256"/>
0031	</KeyBlock>
0032	</PrivateKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="2"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="2"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="PublicKey"/>
0065	<TemplateAttribute>
0066	<Attribute>
0067	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0068	<AttributeValue type="Integer" value="Verify"/>
0069	</Attribute>
0070	<Attribute>
0071	<AttributeName type="TextString" value="Link"/>
0072	<AttributeValue>

0073	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0074	<LinkedObjectIdentifier type="TextString"
0075	value="\$UNIQUE_IDENTIFIER_0"/>
0076	</AttributeValue>
0077	</Attribute>
0078	<AttributeName type="TextString" value="x-ID"/>
0079	<AttributeValue type="TextString" value="TC-ECC-3-12-
0080	pubkey1"/>
0081	</Attribute>
0082	</TemplateAttribute>
0083	<PublicKey>
0084	<KeyBlock>
0085	<KeyFormatType type="Enumeration" value="X_509"/>
0086	<KeyValue>
0087	<KeyMaterial type="ByteString"
0088	value="3056301006072a8648ce3d020106052b8104000a03420004dab5d3c253113
0089	db414abfc1c0ebf5a02559e656aa1c8b0aa8d870aa0324cda4899925eale6dbc259a
0090	6c7825cf46592ac7594cc40bd604b728d88b636f317d366"/>
0091	</KeyValue>
0092	<CryptographicAlgorithm type="Enumeration" value="EC"/>
0093	<CryptographicLength type="Integer" value="256"/>
0094	</KeyBlock>
0095	</PublicKey>
0096	</RequestPayload>
0097	</BatchItem>
0098	</RequestMessage>
0099	<ResponseMessage>
0100	<ResponseHeader>
0101	<ProtocolVersion>
0102	<ProtocolVersionMajor type="Integer" value="1"/>
0103	<ProtocolVersionMinor type="Integer" value="2"/>
0104	</ProtocolVersion>
0105	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0106	<BatchCount type="Integer" value="1"/>
0107	</ResponseHeader>
0108	<BatchItem>
0109	<Operation type="Enumeration" value="Register"/>
0110	<ResultStatus type="Enumeration" value="Success"/>
0111	<ResponsePayload>
0112	<UniqueIdentifier type="TextString"
0113	value="\$UNIQUE_IDENTIFIER_1"/>
0114	</ResponsePayload>
0115	</BatchItem>
0116	</ResponseMessage>
0117	# TIME 2
0118	<RequestMessage>
0119	<RequestHeader>
0120	<ProtocolVersion>
0121	<ProtocolVersionMajor type="Integer" value="1"/>
0122	<ProtocolVersionMinor type="Integer" value="2"/>
	</ProtocolVersion>
	<BatchCount type="Integer" value="1"/>
	</RequestHeader>
	<BatchItem>
	<Operation type="Enumeration" value="Register"/>
	<RequestPayload>

0123	<ObjectType type="Enumeration" value="Certificate"/>
0124	<TemplateAttribute>
0125	<Attribute>
0126	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0127	<AttributeValue type="Integer" value="Verify Sign"/>
0128	</Attribute>
0129	<Attribute>
0130	<AttributeName type="TextString" value="Link"/>
0131	<AttributeValue>
0132	<LinkType type="Enumeration" value="PublicKeyLink"/>
0133	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0134	</AttributeValue>
0135	</Attribute>
0136	<Attribute>
0137	<AttributeName type="TextString" value="x-ID"/>
0138	<AttributeValue type="TextString" value="TC-ECC-3-12-cert1"/>
0139	</Attribute>
0140	</TemplateAttribute>
0141	<Certificate>
0142	<CertificateType type="Enumeration" value="X_509"/>
0143	<CertificateValue type="ByteString" value="308201d53082017aa003020102020900ec0b7402196d5295300a06082a8648ce3d0403023048310b3009060355040613025553310d300b060355040a0c0454455354310e300c060355040b0c054f41534953311a301806035504030c114b4d49502d45432d736563703235366b31301e170d3133303632353130333331315a170d3233303632333130333331315a3048310b3009060355040613025553310d300b060355040a0c0454455354310e300c060355040b0c054f41534953311a301806035504030c114b4d49502d45432d736563703235366b313056301006072a8648ce3d020106052b810400a03420004dab5d3c253113db414abfc1c0ebf5a02559e656aa1c8b0aa8d870aa0324cda4899925ea1e6dbc259a6c7825cf46592ac7594cc40bd604b728d88b636f317d366a350304e301d0603551d0e04160414a098d4bba8817f7e95068c875fbec850b3e177a0301f0603551d23041830168014a098d4bba8817f7e95068c875fbec850b3e177a0300c0603551d13040530030101ff300a06082a8648ce3d0403020349003046022100e9cd14b63e3e57dd26ddfb77a3ed1d05b3721454f617509dff3b9af02d4f5ae022100c9afef9344b8f8b12c525b4618dc3621bce7f8b390ac01ffbe686cc7641c76bb"/>
0144	</Certificate>
0145	</RequestPayload>
0146	</BatchItem>
0147	</RequestMessage>
0148	<ResponseMessage>
0149	<ResponseHeader>
0150	<ProtocolVersion>
0151	<ProtocolVersionMajor type="Integer" value="1"/>
0152	<ProtocolVersionMinor type="Integer" value="2"/>
0153	</ProtocolVersion>
0154	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0155	<BatchCount type="Integer" value="1"/>
0156	</ResponseHeader>
0157	<BatchItem>
0158	<Operation type="Enumeration" value="Register"/>
0159	<ResultStatus type="Enumeration" value="Success"/>
0160	<ResponsePayload>
0161	<UniqueIdentifier type="TextString"

0162	value="\$UNIQUE_IDENTIFIER_2"/>
0163	</ResponsePayload>
0164	</BatchItem>
0164	</ResponseMessage>
0165	# TIME 3
0165	<RequestMessage>
0166	<RequestHeader>
0167	<ProtocolVersion>
0168	<ProtocolVersionMajor type="Integer" value="1"/>
0169	<ProtocolVersionMinor type="Integer" value="2"/>
0170	</ProtocolVersion>
0171	<BatchCount type="Integer" value="2"/>
0172	</RequestHeader>
0173	<BatchItem>
0174	<Operation type="Enumeration" value="AddAttribute"/>
0175	<UniqueBatchItemID type="ByteString" value="01"/>
0176	<RequestPayload>
0177	<UniqueIdentifier type="TextString"
0178	value="\$UNIQUE_IDENTIFIER_0"/>
0178	<Attribute>
0179	<AttributeName type="TextString" value="Link"/>
0180	<AttributeValue>
0181	<LinkType type="Enumeration" value="PublicKeyLink"/>
0182	<LinkedObjectIdentifier type="TextString"
0183	value="\$UNIQUE_IDENTIFIER_1"/>
0184	</AttributeValue>
0185	</Attribute>
0186	</RequestPayload>
0187	</BatchItem>
0188	<BatchItem>
0188	<Operation type="Enumeration" value="AddAttribute"/>
0189	<UniqueBatchItemID type="ByteString" value="02"/>
0190	<RequestPayload>
0191	<UniqueIdentifier type="TextString"
0192	value="\$UNIQUE_IDENTIFIER_0"/>
0192	<Attribute>
0193	<AttributeName type="TextString" value="Link"/>
0194	<AttributeValue>
0195	<LinkType type="Enumeration" value="CertificateLink"/>
0196	<LinkedObjectIdentifier type="TextString"
0197	value="\$UNIQUE_IDENTIFIER_2"/>
0198	</AttributeValue>
0199	</Attribute>
0200	</RequestPayload>
0201	</BatchItem>
0201	</RequestMessage>
0202	<ResponseMessage>
0203	<ResponseHeader>
0204	<ProtocolVersion>
0205	<ProtocolVersionMajor type="Integer" value="1"/>
0206	<ProtocolVersionMinor type="Integer" value="2"/>
0207	</ProtocolVersion>
0208	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0209	<BatchCount type="Integer" value="2"/>
0210	</ResponseHeader>
0211	<BatchItem>
0212	<Operation type="Enumeration" value="AddAttribute"/>

0213	<UniqueBatchItemID type="ByteString" value="01"/>
0214	<ResultStatus type="Enumeration" value="Success"/>
0215	<ResponsePayload>
0216	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0217	<Attribute>
0218	<AttributeName type="TextString" value="Link"/>
0219	<AttributeValue>
0220	<LinkType type="Enumeration" value="PublicKeyLink"/>
0221	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0222	</AttributeValue>
0223	</Attribute>
0224	</ResponsePayload>
0225	</BatchItem>
0226	<BatchItem>
0227	<Operation type="Enumeration" value="AddAttribute"/>
0228	<UniqueBatchItemID type="ByteString" value="02"/>
0229	<ResultStatus type="Enumeration" value="Success"/>
0230	<ResponsePayload>
0231	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0232	<Attribute>
0233	<AttributeName type="TextString" value="Link"/>
0234	<AttributeIndex type="Integer" value="1"/>
0235	<AttributeValue>
0236	<LinkType type="Enumeration" value="CertificateLink"/>
0237	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0238	</AttributeValue>
0239	</Attribute>
0240	</ResponsePayload>
0241	</BatchItem>
0242	</ResponseMessage>
	# TIME 4
0243	<RequestMessage>
0244	<RequestHeader>
0245	<ProtocolVersion>
0246	<ProtocolVersionMajor type="Integer" value="1"/>
0247	<ProtocolVersionMinor type="Integer" value="2"/>
0248	</ProtocolVersion>
0249	<BatchCount type="Integer" value="1"/>
0250	</RequestHeader>
0251	<BatchItem>
0252	<Operation type="Enumeration" value="GetAttributeList"/>
0253	<RequestPayload>
0254	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0255	</RequestPayload>
0256	</BatchItem>
0257	</RequestMessage>
0258	<ResponseMessage>
0259	<ResponseHeader>
0260	<ProtocolVersion>
0261	<ProtocolVersionMajor type="Integer" value="1"/>
0262	<ProtocolVersionMinor type="Integer" value="2"/>
0263	</ProtocolVersion>

0264	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0265	<BatchCount type="Integer" value="1"/>
0266	</ResponseHeader>
0267	<BatchItem>
0268	<Operation type="Enumeration" value="GetAttributeList"/>
0269	<ResultStatus type="Enumeration" value="Success"/>
0270	<ResponsePayload>
0271	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0272	<AttributeName type="TextString" value="x-ID"/>
0273	<AttributeName type="TextString" value="Unique Identifier"/>
0274	<AttributeName type="TextString" value="Object Type"/>
0275	<AttributeName type="TextString" value="Certificate Type"/>
0276	<AttributeName type="TextString" value="Certificate
	Identifier"/>
0277	<AttributeName type="TextString" value="Certificate Issuer"/>
0278	<AttributeName type="TextString" value="Certificate Length"/>
0279	<AttributeName type="TextString" value="Certificate Subject"/>
0280	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0281	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0282	<AttributeName type="TextString" value="Digest"/>
0283	<AttributeName type="TextString" value="Digital Signature
	Algorithm"/>
0284	<AttributeName type="TextString" value="Fresh"/>
0285	<AttributeName type="TextString" value="Initial Date"/>
0286	<AttributeName type="TextString" value="Last Change Date"/>
0287	<AttributeName type="TextString" value="Lease Time"/>
0288	<AttributeName type="TextString" value="Link"/>
0289	<AttributeName type="TextString" value="State"/>
0290	<AttributeName type="TextString" value="X.509 Certificate
	Identifier"/>
0291	<AttributeName type="TextString" value="X.509 Certificate
	Issuer"/>
0292	<AttributeName type="TextString" value="X.509 Certificate
	Subject"/>
0293	</ResponsePayload>
0294	</BatchItem>
0295	</ResponseMessage>
	# TIME 5
0296	<RequestMessage>
0297	<RequestHeader>
0298	<ProtocolVersion>
0299	<ProtocolVersionMajor type="Integer" value="1"/>
0300	<ProtocolVersionMinor type="Integer" value="2"/>
0301	</ProtocolVersion>
0302	<BatchCount type="Integer" value="1"/>
0303	</RequestHeader>
0304	<BatchItem>
0305	<Operation type="Enumeration" value="GetAttributes"/>
0306	<RequestPayload>
0307	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0308	<AttributeName type="TextString" value="Digital Signature
	Algorithm"/>
0309	<AttributeName type="TextString" value="X.509 Certificate

0310	Identifier"/>
0311	<AttributeName type="TextString" value="X.509 Certificate
0312	Issuer"/>
0313	<AttributeName type="TextString" value="X.509 Certificate
0314	Subject"/>
0315	</RequestPayload>
0316	</BatchItem>
0317	</RequestMessage>
0318	<ResponseMessage>
0319	<ResponseHeader>
0320	<ProtocolVersion>
0321	<ProtocolVersionMajor type="Integer" value="1"/>
0322	<ProtocolVersionMinor type="Integer" value="2"/>
0323	</ProtocolVersion>
0324	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0325	<BatchCount type="Integer" value="1"/>
0326	</ResponseHeader>
0327	<BatchItem>
0328	<Operation type="Enumeration" value="GetAttributes"/>
0329	<ResultStatus type="Enumeration" value="Success"/>
0330	<ResponsePayload>
0331	<UniqueIdentifier type="TextString"
0332	value="\$UNIQUE_IDENTIFIER_2"/>
0333	<Attribute>
0334	<AttributeName type="TextString" value="Digital Signature
0335	Algorithm"/>
0336	<AttributeValue type="Enumeration" value="ECDSAWithSHA256"/>
0337	</Attribute>
0338	<Attribute>
0339	<AttributeName type="TextString" value="X.509 Certificate
0340	Identifier"/>
0341	<AttributeValue>
0342	<IssuerDistinguishedName type="ByteString"
0343	value="3048310b3009060355040613025553310d300b060355040a0c04544553543
0344	10e300c060355040b0c054f41534953311a301806035504030c114b4d49502d45432
0345	d736563703235366b31"/>
0346	<CertificateSerialNumber type="ByteString"
0347	value="020900ec0b7402196d5295"/>
0348	</AttributeValue>
0349	</Attribute>
0350	<Attribute>
0351	<AttributeName type="TextString" value="X.509 Certificate
0352	Issuer"/>
0353	<AttributeValue>
0354	<IssuerDistinguishedName type="ByteString"
0355	value="3048310b3009060355040613025553310d300b060355040a0c04544553543
0356	10e300c060355040b0c054f41534953311a301806035504030c114b4d49502d45432
0357	d736563703235366b31"/>
0358	</AttributeValue>
0359	</Attribute>
0360	<Attribute>
0361	<AttributeName type="TextString" value="X.509 Certificate
0362	Subject"/>
0363	<AttributeValue>
0364	<SubjectDistinguishedName type="ByteString"
0365	value="3048310b3009060355040613025553310d300b060355040a0c04544553543
0366	10e300c060355040b0c054f41534953311a301806035504030c114b4d49502d45432
0367	d736563703235366b31"/>

0350	d736563703235366b31"/>
0351	</AttributeValue>
0352	</Attribute>
0353	</ResponsePayload>
0354	</BatchItem>
0355	</ResponseMessage>
# TIME 6	
0355	<RequestMessage>
0356	<RequestHeader>
0357	<ProtocolVersion>
0358	<ProtocolVersionMajor type="Integer" value="1"/>
0359	<ProtocolVersionMinor type="Integer" value="2"/>
0360	</ProtocolVersion>
0361	<BatchCount type="Integer" value="1"/>
0362	</RequestHeader>
0363	<BatchItem>
0364	<Operation type="Enumeration" value="Locate"/>
0365	<RequestPayload>
0366	<Attribute>
0367	<AttributeName type="TextString" value="Object Type"/>
0368	<AttributeValue type="Enumeration" value="PublicKey"/>
0369	</Attribute>
0370	<Attribute>
0371	<AttributeName type="TextString" value="Link"/>
0372	<AttributeValue>
0373	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0374	<LinkedObjectIdentifier type="TextString"
0375	value="\$UNIQUE_IDENTIFIER_0"/>
0376	</AttributeValue>
0377	</Attribute>
0378	</RequestPayload>
0379	</BatchItem>
0380	</RequestMessage>
0381	<ResponseMessage>
0382	<ResponseHeader>
0383	<ProtocolVersion>
0384	<ProtocolVersionMajor type="Integer" value="1"/>
0385	<ProtocolVersionMinor type="Integer" value="2"/>
0386	</ProtocolVersion>
0387	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0388	<BatchCount type="Integer" value="1"/>
0389	</ResponseHeader>
0390	<BatchItem>
0391	<Operation type="Enumeration" value="Locate"/>
0392	<ResultStatus type="Enumeration" value="Success"/>
0393	<ResponsePayload>
0394	<UniqueIdentifier type="TextString"
0395	value="\$UNIQUE_IDENTIFIER_1"/>
0396	</ResponsePayload>
0397	</BatchItem>
0398	</ResponseMessage>
# TIME 7	
0397	<RequestMessage>
0398	<RequestHeader>
0399	<ProtocolVersion>
0400	<ProtocolVersionMajor type="Integer" value="1"/>

0401	<ProtocolVersionMinor type="Integer" value="2"/>
0402	</ProtocolVersion>
0403	<BatchCount type="Integer" value="1"/>
0404	</RequestHeader>
0405	<BatchItem>
0406	<Operation type="Enumeration" value="Locate"/>
0407	<RequestPayload>
0408	<Attribute>
0409	<AttributeName type="TextString" value="Object Type"/>
0410	<AttributeValue type="Enumeration" value="PrivateKey"/>
0411	</Attribute>
0412	<Attribute>
0413	<AttributeName type="TextString" value="Link"/>
0414	<AttributeValue>
0415	<LinkType type="Enumeration" value="PublicKeyLink"/>
0416	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0417	</AttributeValue>
0418	</Attribute>
0419	</RequestPayload>
0420	</BatchItem>
0421	</RequestMessage>
0422	<ResponseMessage>
0423	<ResponseHeader>
0424	<ProtocolVersion>
0425	<ProtocolVersionMajor type="Integer" value="1"/>
0426	<ProtocolVersionMinor type="Integer" value="2"/>
0427	</ProtocolVersion>
0428	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0429	<BatchCount type="Integer" value="1"/>
0430	</ResponseHeader>
0431	<BatchItem>
0432	<Operation type="Enumeration" value="Locate"/>
0433	<ResultStatus type="Enumeration" value="Success"/>
0434	<ResponsePayload>
0435	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0436	</ResponsePayload>
0437	</BatchItem>
0438	</ResponseMessage>
	# TIME 8
0439	<RequestMessage>
0440	<RequestHeader>
0441	<ProtocolVersion>
0442	<ProtocolVersionMajor type="Integer" value="1"/>
0443	<ProtocolVersionMinor type="Integer" value="2"/>
0444	</ProtocolVersion>
0445	<BatchCount type="Integer" value="1"/>
0446	</RequestHeader>
0447	<BatchItem>
0448	<Operation type="Enumeration" value="Get"/>
0449	<RequestPayload>
0450	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0451	</RequestPayload>
0452	</BatchItem>
0453	</RequestMessage>

0454	<ResponseMessage>
0455	<ResponseHeader>
0456	<ProtocolVersion>
0457	<ProtocolVersionMajor type="Integer" value="1"/>
0458	<ProtocolVersionMinor type="Integer" value="2"/>
0459	</ProtocolVersion>
0460	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0461	<BatchCount type="Integer" value="1"/>
0462	</ResponseHeader>
0463	<BatchItem>
0464	<Operation type="Enumeration" value="Get"/>
0465	<ResultStatus type="Enumeration" value="Success"/>
0466	<ResponsePayload>
0467	<ObjectType type="Enumeration" value="PrivateKey"/>
0468	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0469	<PrivateKey>
0470	<KeyBlock>
0471	<KeyFormatType type="Enumeration" value="ECPrivateKey"/>
0472	<KeyValue>
0473	<KeyMaterial type="ByteString"
	value="30740201010420db4d128c30ca309e62c4019758c00ba244dd64d9bf52a31
	078866b8a00c19c68a00706052b8104000aa14403420004dab5d3c253113db414abf
	c1c0ebf5a02559e656aa1c8b0aa8d870aa0324cda4899925eale6dbc259a6c7825cf
	46592ac7594cc40bd604b728d88b636f317d366"/>
0474	</KeyValue>
0475	<CryptographicAlgorithm type="Enumeration" value="EC"/>
0476	<CryptographicLength type="Integer" value="256"/>
0477	</KeyBlock>
0478	</PrivateKey>
0479	</ResponsePayload>
0480	</BatchItem>
0481	</ResponseMessage>
	# TIME 9
0482	<RequestMessage>
0483	<RequestHeader>
0484	<ProtocolVersion>
0485	<ProtocolVersionMajor type="Integer" value="1"/>
0486	<ProtocolVersionMinor type="Integer" value="2"/>
0487	</ProtocolVersion>
0488	<BatchCount type="Integer" value="1"/>
0489	</RequestHeader>
0490	<BatchItem>
0491	<Operation type="Enumeration" value="Get"/>
0492	<RequestPayload>
0493	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0494	</RequestPayload>
0495	</BatchItem>
0496	</RequestMessage>
0497	<ResponseMessage>
0498	<ResponseHeader>
0499	<ProtocolVersion>
0500	<ProtocolVersionMajor type="Integer" value="1"/>
0501	<ProtocolVersionMinor type="Integer" value="2"/>
0502	</ProtocolVersion>
0503	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>

0504	<BatchCount type="Integer" value="1"/>
0505	</ResponseHeader>
0506	<BatchItem>
0507	<Operation type="Enumeration" value="Get"/>
0508	<ResultStatus type="Enumeration" value="Success"/>
0509	<ResponsePayload>
0510	<ObjectType type="Enumeration" value="PublicKey"/>
0511	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0512	<PublicKey>
0513	<KeyBlock>
0514	<KeyFormatType type="Enumeration" value="X_509"/>
0515	<KeyValue>
0516	<KeyMaterial type="ByteString"
	value="3056301006072a8648ce3d020106052b8104000a03420004dab5d3c253113
	db414abfc1c0ebf5a02559e656aa1c8b0aa8d870aa0324cda4899925eale6dbc259a
	6c7825cf46592ac7594cc40bd604b728d88b636f317d366"/>
0517	</KeyValue>
0518	<CryptographicAlgorithm type="Enumeration" value="EC"/>
0519	<CryptographicLength type="Integer" value="256"/>
0520	</KeyBlock>
0521	</PublicKey>
0522	</ResponsePayload>
0523	</BatchItem>
0524	</ResponseMessage>
	# TIME 10
0525	<RequestMessage>
0526	<RequestHeader>
0527	<ProtocolVersion>
0528	<ProtocolVersionMajor type="Integer" value="1"/>
0529	<ProtocolVersionMinor type="Integer" value="2"/>
0530	</ProtocolVersion>
0531	<BatchCount type="Integer" value="1"/>
0532	</RequestHeader>
0533	<BatchItem>
0534	<Operation type="Enumeration" value="Destroy"/>
0535	<RequestPayload>
0536	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0537	</RequestPayload>
0538	</BatchItem>
0539	</RequestMessage>
0540	<ResponseMessage>
0541	<ResponseHeader>
0542	<ProtocolVersion>
0543	<ProtocolVersionMajor type="Integer" value="1"/>
0544	<ProtocolVersionMinor type="Integer" value="2"/>
0545	</ProtocolVersion>
0546	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0547	<BatchCount type="Integer" value="1"/>
0548	</ResponseHeader>
0549	<BatchItem>
0550	<Operation type="Enumeration" value="Destroy"/>
0551	<ResultStatus type="Enumeration" value="Success"/>
0552	<ResponsePayload>
0553	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0554	</ResponsePayload>
0555	</BatchItem>
0556	</ResponseMessage>
# TIME 11	
0557	<RequestMessage>
0558	<RequestHeader>
0559	<ProtocolVersion>
0560	<ProtocolVersionMajor type="Integer" value="1"/>
0561	<ProtocolVersionMinor type="Integer" value="2"/>
0562	</ProtocolVersion>
0563	<BatchCount type="Integer" value="1"/>
0564	</RequestHeader>
0565	<BatchItem>
0566	<Operation type="Enumeration" value="Destroy"/>
0567	<RequestPayload>
0568	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0569	</RequestPayload>
0570	</BatchItem>
0571	</RequestMessage>
0572	<ResponseMessage>
0573	<ResponseHeader>
0574	<ProtocolVersion>
0575	<ProtocolVersionMajor type="Integer" value="1"/>
0576	<ProtocolVersionMinor type="Integer" value="2"/>
0577	</ProtocolVersion>
0578	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0579	<BatchCount type="Integer" value="1"/>
0580	</ResponseHeader>
0581	<BatchItem>
0582	<Operation type="Enumeration" value="Destroy"/>
0583	<ResultStatus type="Enumeration" value="Success"/>
0584	<ResponsePayload>
0585	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0586	</ResponsePayload>
0587	</BatchItem>
0588	</ResponseMessage>
# TIME 12	
0589	<RequestMessage>
0590	<RequestHeader>
0591	<ProtocolVersion>
0592	<ProtocolVersionMajor type="Integer" value="1"/>
0593	<ProtocolVersionMinor type="Integer" value="2"/>
0594	</ProtocolVersion>
0595	<BatchCount type="Integer" value="1"/>
0596	</RequestHeader>
0597	<BatchItem>
0598	<Operation type="Enumeration" value="Destroy"/>
0599	<RequestPayload>
0600	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_2"/>
0601	</RequestPayload>
0602	</BatchItem>
0603	</RequestMessage>
0604	<ResponseMessage>

```
0605 <ResponseHeader>
0606   <ProtocolVersion>
0607     <ProtocolVersionMajor type="Integer" value="1"/>
0608     <ProtocolVersionMinor type="Integer" value="2"/>
0609   </ProtocolVersion>
0610   <TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0611   <BatchCount type="Integer" value="1"/>
0612 </ResponseHeader>
0613 <BatchItem>
0614   <Operation type="Enumeration" value="Destroy"/>
0615   <ResultStatus type="Enumeration" value="Success"/>
0616   <ResponsePayload>
0617     <UniqueIdentifier type="TextString"
0618       value="$UNIQUE_IDENTIFIER_2"/>
0619   </ResponsePayload>
0620 </BatchItem>
0621 </ResponseMessage>
```

1143

1144 2.3.42 TC-PGP-1-12 - Register PGP Key - RSA

1145 Register a PGP public and private key block. Add the appropriate links between the registered
1146 objects. Make sure everything was registered and the attributes set correctly by listing and
1147 retrieving the attributes. Get the keys, and finally destroy all the registered objects.

1148 Note: the ascii armored keys are:

1149

1150 -----BEGIN PGP PUBLIC KEY BLOCK-----

1151

```
1152 mQENBFHA/dQBCADged9e6tib8klFhPpwSni1JseckqjSL5wT1QKKmJMMRyI1Ru5R
1153 rJSBcRwjOoaaRdavnZEJ1xujU32Zj+2H2sqS6sSnizCNnkF5HCWO2J3b5M5vPkdG
1154 PYqrlcv7lvP8P0wjctOueDxnSgx6Ijn4QDjd+tLnTxTK8U0YhZsGZCwu+3S6kwhg
1155 xlWSz+39oP0kT58+Jvnlx8vowtVqZ+7npqrMOojIVedFSfk+z2Co1UObj6l+xzTt
1156 1kqQZfXC/yyMAFWTKcPEy/KCw6u2bzvouZMM3dkgfU/AuqqpKSBABH0Z/blnC2Ty
1157 QdSuOKxzgcyIBcW5wRnKtjstWW9Ycf/jI6EtABEBAAG0T0tNSVAgVVFuIjBSU0Eg
1158 KE9BU01TIETleSBNYW5hZ2VtZW50IEludGVyb3BlcmFiaWxpdHkgUHJvdG9jb2wp
1159 IDxrbWlwM0BrbWlwLmNvbT6JATYEEwECACAFAlHA/dQCGy8GCwkIBwMCBBUCCAME
1160 FgIDAQIeAQIXgAAKCRaKDBezbMoNjkd1B/9PLphGbxPO27yeyX9CnZ/ZsRPbGVHW
1161 XmMR2riXoBxB1FR4dlV/Xngrevk4SZBFXIKx2w0hppSQVgrBKYCms/hFCKScVaVb
1162 cNQy8L0Q5TNjFPzxyUAP8MLUFu+Rr5OIiPIYuGFM26QnTBfDFOhDh7Mvj2wWUuZ
1163 b2oV6i6gj97mfyNJ1mJHfr+MbO6hBebAPvns6kYivSDyrGr06cpUatoeh0+2YN25
1164 XdEmDk0bqy9kpJMwHjjULkwnsFjbv+KhXxl2jG6mleqNiAiUVPftXY4yKmtfiBZa
1165 4J0j04omkU8Jj4fvlkOo2o6kbs+htqD+J5WHxmX1TosgrfzuV8z5Mt7U
1166 =nVOy
```

1167 -----END PGP PUBLIC KEY BLOCK-----

1168

1169 -----BEGIN PGP PRIVATE KEY BLOCK-----

1170

```
1171 lQO+BFHA/dQBCADged9e6tib8klFhPpwSni1JseckqjSL5wT1QKKmJMMRyI1Ru5R
1172 rJSBcRwjOoaaRdavnZEJ1xujU32Zj+2H2sqS6sSnizCNnkF5HCWO2J3b5M5vPkdG
1173 PYqrlcv7lvP8P0wjctOueDxnSgx6Ijn4QDjd+tLnTxTK8U0YhZsGZCwu+3S6kwhg
1174 xlWSz+39oP0kT58+Jvnlx8vowtVqZ+7npqrMOojIVedFSfk+z2Co1UObj6l+xzTt
1175 1kqQZfXC/yyMAFWTKcPEy/KCw6u2bzvouZMM3dkgfU/AuqqpKSBABH0Z/blnC2Ty
1176 QdSuOKxzgcyIBcW5wRnKtjstWW9Ycf/jI6EtABEBAAH+AwMCKJbXYz63HjZgp520
```

```
1177 SnT31jWMxLnE+A4SNw6COTS/6brgHJVCkPYnORZQDpoakJg+F8HWqx+movO6l0UN
1178 dj0gqyR4NF/2tMvgKTT0FMdr7LriSLQsCCh5EwqXm2vnfv9p4qfL0BtjtACv+5XZ
1179 DZXYdaFtbSgE8bbLe/AFQLqPOdWotoLCH/ED0R54Q+VciaZmogiAVbwIjYkNWxMV
1180 1gSETpwL74Fzgu0DigFJpE7SyhqRSdSkMXlyAmZwg0uoLDCTn8aYrSEjrBsy7Rt
1181 337AsWSSMznFtyzYbV1PhtHh0GhHBdUro/4Ad5o76Mset3BclM6UAg6UMSbjC/vv
1182 U6yPyje8yepvCfov/G7tSQbiIEwSOXUxamm2etvno3YBMxm5l7x9ZP7Zfz8+zcVJ
1183 mAVxS5/QQGV9EMFOGGYWQ5ZcTckQ+eGnzZMQmB6jVWahqU8iXM3/g5Y8IP5i87OY
1184 zLHhybp24RXYoOTiB2rxulzmMVUYKlgd6gNlHdysQM4K1deHw8R37e/NKJrmGX+3
1185 psHINp5EJqnB3JfQ3p7A7CMhcJ5Phx3m9UmCrKlyGMJdFC1+tN2P5QSA8dAchgvB
1186 C0L4oZ83CCZUmmM4ljI+BoscLOgyKSPmsplzrz4L7TrHM8K5zFoXHkZzPPWZTM25
1187 ilTywogsUhqXe9wyaw6PHTHBy+clhvXcHQffFwfqeyKe05nGuKBZcpqsXJg/Zg1
1188 rqKmrU2azd2mGtYikQmxlkr+IO9dD58B7gOakyZAHe5NauT90CtL67qjAX2+aJRb
1189 uu2FLD1yUBMjpfUq3a5sQl6qo9/rC8iknDA/hFBpID3LRqDJGtYafPv8o6FjZH1U
1190 rUCx80Y0rmNelV65XPtE8+so2H1/hgWHERdNspiTsGESfSE1RxuuNS+iFW/gSy3C
1191 ErRPS01JUCBVU0VSIFJTQSAoT0FTSVMgS2V5IE1hbmFnZWl1bnQgSW50ZXJvcGVy
1192 YWJpbG10eSBQcm90b2NvbCkgPGttaXAzQGttaXAuY29tPokBNgQTAQIAIAUCUCd9
1193 1AIbLwYLCQgHAWIEFQIIAwQWAgMBAh4BAheAAAJECQMF7Nsyg0mR3UH/08umEZv
1194 E87bvJ7Jf0Kdn9mxE9sZUdZeYxHauJegFchUVHh2VX9eeCt6+ThJkFcUgrHbDSGm
1195 lJBWCsEpgKaz+EUipJxVpVtwlDLwvRDlM2MU/PHJQA/wwtQW75Gvk4iI8hi4YUzb
1196 pCdMF8MU6EOHsy+OPbBZS5lvahXqLqCP3uZ/I0nWYkd+v4xs7qEF5sA++ezqRiK9
1197 IPKsavTpylRq2h6HT7Zg3bld0SYOTRurL2SkkzAeONQuTCewWNU/4qFfGXaMbqaU
1198 So2ICJRU9+ldjjIqZN+IFlrgnSPTiiaRTwmPh++WQ6jajqRuz6G2oP4nlyFGzfVO
1199 iyCt/O5XzPky3tQ=
1200 =vd7s
1201 -----END PGP PRIVATE KEY BLOCK-----
```

#	TIME	0
0001	<RequestMessage>	
0002	<RequestHeader>	
0003	<ProtocolVersion>	
0004	<ProtocolVersionMajor	type="Integer" value="1"/>
0005	<ProtocolVersionMinor	type="Integer" value="2"/>
0006	</ProtocolVersion>	
0007	<BatchCount	type="Integer" value="1"/>
0008	</RequestHeader>	
0009	<BatchItem>	
0010	<Operation	type="Enumeration" value="Register"/>
0011	<RequestPayload>	
0012	<ObjectType	type="Enumeration" value="PGPKey"/>
0013	<TemplateAttribute>	
0014	<Attribute>	
0015	<AttributeName	type="TextString" value="x-ID"/>
0016	<AttributeValue	type="TextString" value="TC-PGP-1-12- pubkey1"/>
0017	</Attribute>	
0018	<Attribute>	
0019	<AttributeName	type="TextString" value="Alternative Name"/>
0020	<AttributeValue>	
0021	<AlternativeNameValue	type="TextString" value="kmip3@kmip.com"/>
0022	<AlternativeNameType	type="Enumeration" value="UninterpretedTextString"/>
0023	</AttributeValue>	
0024	</Attribute>	
0025	<Attribute>	
0026	<AttributeName	type="TextString" value="Alternative Name"/>
0027	<AttributeValue>	
0028	<AlternativeNameValue	type="TextString" value="KMIP USER


```

0029      <AlternativeNameType type="Enumeration"
value="UninterpretedTextString"/>
0030      </AttributeValue>
0031      </Attribute>
0032      <Attribute>
0033          <AttributeName type="TextString" value="Alternative Name"/>
0034          <AttributeValue>
0035              <AlternativeNameValue type="TextString" value="6CCA0D26"/>
0036              <AlternativeNameType type="Enumeration"
value="ObjectSerialNumber"/>
0037              </AttributeValue>
0038              </Attribute>
0039              <Attribute>
0040                  <AttributeName type="TextString" value="Alternative Name"/>
0041                  <AttributeValue>
0042                      <AlternativeNameValue type="TextString"
value="240C17B36CCA0D26"/>
0043                      <AlternativeNameType type="Enumeration"
value="ObjectSerialNumber"/>
0044                      </AttributeValue>
0045                      </Attribute>
0046                      </TemplateAttribute>
0047                      <PGPKey>
0048                          <PGPKeyVersion type="Integer" value="4"/>
0049                          <KeyBlock>
0050                              <KeyFormatType type="Enumeration" value="Raw"/>
0051                              <KeyValue>
0052                                  <KeyMaterial type="ByteString"
value="2d2d2d2d2d2d424547494e20504750205055424c4943204b455920424c4f434
b2d2d2d2d2d0a0a6d51454e424648412f645142434144676564396536746962386b6
c4668507077536e69314a7365636b716a534c35775431514b4b6d4a4d4d527949315
27535520a724a53426352776a4f6f6161526461766e5a454a3178756a5533325a6a2
b3248327371733673536e697a434e6e6b46354843574f324a3362354d3576506b644
70a505971726c6376376c7650385030776a63544f756544786e53677836496a6e345
1446a642b744c6e5478544b38553059687a73475a4377752b3353366b7768670a786
c57537a2b33396f50306b5435382b4a766e6c7838766f777476715a2b376e7071724
d4f6f6a495665644653666b2b7a32436f31554f626a366c2b787a54740a316b71515
a6658432f79794d414677544b635045792f4b4377367532627a766f755a4d4d33646
b6766552f41757171704b5342414248305a2f626c6e433254790a516453754f4b787
a676379494263573577526e4b746a73745757395943662f6a4936457441424542414
147305430744e5356416756564e4655694253553045670a4b45394255306c5449457
46c6553424e595735685a3256745a57353049456c75644756796233426c636d46696
157787064486b6755484a766447396a623277700a4944787262576c774d304272625
76c774c6d4e766254364a415459454577454341434146416c48412f6451434779384
743776b4942774d434242554343414d450a4667494441514965415149586741414b4
352416b4442657a624d6f4e4a6b6431422f39504c7068476278504f3237796579583
9436e5a2f5a73525062475648570a586d4d52327269586f42584231465234646c562
f586e677265766b34535a425846494b783277306870705351566772424b59436d732
f6846434b5363566156620a634e5179384c305135544e6a46507a7879554150384d4
c5546752b5272354f49695049597547464d3236516e54426644464f684468374d766
a6a32775755755a0a62326f56366936676a39376d66794e4a316d4a4866722b4d624
f36684265624150766e73366b5969765347092477230663705561746f6568302b3
2594e32350a5864456d446b30627179396b704a4d77486a6a554c6b776e73466a627
62b4b6858786c326a47366d6c45714e6941695556506674585934794b6d546669425
a610a344a306a30346f6d6b55384a6a3466766c6b4f6f326f366b62732b687471444

```

0053	b4a355748786d5831546f736772667a7556387a354d7437550a3d6e564f790a2d2d2d2d2d454e4420504750205055424c4943204b455920424c4f434b2d2d2d2d2d0a"/>
0054	</KeyValue>
0055	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0056	<CryptographicLength type="Integer" value="2048"/>
0057	</KeyBlock>
0058	</PGPKey>
0059	</RequestPayload>
0060	</BatchItem>
0061	</RequestMessage>
0062	<ResponseMessage>
0063	<ResponseHeader>
0064	<ProtocolVersion>
0065	<ProtocolVersionMajor type="Integer" value="1"/>
0066	<ProtocolVersionMinor type="Integer" value="2"/>
0067	</ProtocolVersion>
0068	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0069	<BatchCount type="Integer" value="1"/>
0070	</ResponseHeader>
0071	<BatchItem>
0072	<Operation type="Enumeration" value="Register"/>
0073	<ResultStatus type="Enumeration" value="Success"/>
0074	<ResponsePayload>
0075	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0076	</ResponsePayload>
0077	</BatchItem>
0078	</ResponseMessage>
0078	# TIME 1
0079	<RequestMessage>
0080	<RequestHeader>
0081	<ProtocolVersion>
0082	<ProtocolVersionMajor type="Integer" value="1"/>
0083	<ProtocolVersionMinor type="Integer" value="2"/>
0084	</ProtocolVersion>
0085	<BatchCount type="Integer" value="1"/>
0086	</RequestHeader>
0087	<BatchItem>
0088	<Operation type="Enumeration" value="Register"/>
0089	<RequestPayload>
0090	<ObjectType type="Enumeration" value="PGPKey"/>
0091	<TemplateAttribute>
0092	<Attribute>
0093	<AttributeName type="TextString" value="x-ID"/>
0094	<AttributeValue type="TextString" value="TC-PGP-1-12-prikey1"/>
0095	</Attribute>
0096	<Attribute>
0097	<AttributeName type="TextString" value="Link"/>
0098	<AttributeValue>
0099	<LinkType type="Enumeration" value="PublicKeyLink"/>
0100	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0101	</AttributeValue>
0102	</Attribute>
0103	</TemplateAttribute>
0103	</PGPKey>

0104	<PGPKeyVersion type="Integer" value="4"/>
0105	<KeyBlock>
0106	<KeyFormatType type="Enumeration" value="Raw"/>
0107	<KeyValue>
0108	<KeyMaterial type="ByteString"
	value="2d2d2d2d2d424547494e205047502050524956415445204b455920424c4f4
	34b2d2d2d2d0a0a6c514f2b424648412f645142434144676564396536746962386
	b6c4668507077536e69314a7365636b716a534c35775431514b4b6d4a4d4d5279493
	1527535520a724a53426352776a4f6f6161526461766e5a454a3178756a5533325a6
	a2b3248327371733673536e697a434e6e6b46354843574f324a3362354d3576506b6
	4470a505971726c6376376c7650385030776a63544f756544786e53677836496a6e3
	451446a642b744c6e5478544b38553059687a73475a4377752b3353366b7768670a7
	86c57537a2b33396f50306b5435382b4a766e6c7838766f777476715a2b376e70717
	24d4f6f6a495665644653666b2b7a32436f31554f626a366c2b787a54740a316b715
	15a6658432f79794d414677544b635045792f4b4377367532627a766f755a4d4d336
	46b6766552f41757171704b5342414248305a2f626c6e433254790a516453754f4b7
	87a676379494263573577526e4b746a73745757395943662f6a49364574414245424
	141482b41774d434b4a6258597a3633486a5a67703532300a536e5433316a574d784
	c6e452b4134534e7736434f54532f36627267484a56436b50596e4f525a5144706f6
	16b4a672b4638485771782b6d6f764f366c30554e0a646a3067717952344e462f327
	44d76674b545430464d6472374c7269534c517343436835457771586d32766e66763
	9703471664c3042746a744143762b35585a0a445a587964614674625367453862624
	c652f4146514c71504f64574f746f4c43482f454430523534512b566369615a6d6f6
	76941566277496a596b4e57784d560a316753455470774c3734467a6775304469674
	64a7045375379687152536444736b4d586c79416d5a776730756f4c4443744e38615
	97253456a724273793752740a33333741735753534d7a6e4674797a5962563150687
	4486830476848426455726f2f344164356f37364d7365743342636c4d36554167365
	54d53626a432f76760a55367950796a65387965707643666f762f473774535162694
	94577534f585578616d6d326574766e6f3359424d786d356c3778395a50375a667a3
	82b7a63564a0a6d41567853352f5151477639454d464f4747595751355a6354636b5
	12b65476e7a5a4d516d42366a5657616871553869584d332f6735593849503569383
	74f590a7a4c486879627032345258794f6f546942327278756c7a6d4d5655594b6c6
	76436674e6c48647973514d344b316465487738523337652f4e4b4a726d47582b330
	a707348494e7035454a716e42334a66513370374137434d68634a35506878336d395
	56d43724b6c79474d4a6446436c2b744e32503551534138644163686776420a43304
	c346f5a383343435a556d6d4d346c6a492b426f73634c4f67794b53506d73706c7a7
	27a344c375472484d384b357a466f58486b5a7a5050575a544d32350a696c5479776
	f67735568715865397779796177365048544842792b6331687658634851666646776
	67165794b654f356e47754b425a63707173584a672f5a67310a72714b6d725532617
	a64326d477459696b516d786c6b522b494f39644435384237674f416b797a4148653
	54e617554393043744c3637716a4158322b614a52620a757532464c44317955424d6
	a7066557133613573516c36716f392f724338696b6e44412f684642704944334c527
	1444a47745961665076386f36466a5a4831550a7255437838305930726d4e656c563
	63558507445382b736f32486c2f686777484552644e7370695473474553665345315
	27875754e532b6946572f67537933430a457252505330314a5543425655305653494
	64a545153416f5430465453564d675332563549453168626d466e5a57316c626e516
	7535735305a584a76634756790a59574a7062476c3065534251636d393062324e766
	2436b67504774746158417a514774746158417559323974506f6b424e67515441514
	94149415543556344390a314149624c77594c4351674841774945465149494177515
	741674d42416834424168654141416f4a4543514d46374e737967306d523355482f3
	038756d455a760a45383762764a374a66304b646e396d784539735a55645a6559784
	861754a6567466348555648683256583965654374362b54684a6b466355677248624
	453476d0a6c4a425743734570674b617a2b455549704a78567056747731444c77765
	2446c4d324d552f50484a51412f7777745157373547766b3469493868693459557a6
	20a7043644d46384d5536454f4873792b4f5062425a53356c76616858714c7143503
	3755a2f49306e57596b642b76347873377145463573412b2b657a7152694b390a495
	04b7361765470796c52713268364854375a6733626c643053594f545275724c32536

0109	b6b7a41654f4e517554436577574e752f347146664758614d627161550a536f32494
0110	34a5255392b31646a6a49715a4e2b49466c72676e5350546969615254776d50682b2
0111	b5751366a616a7152757a3647326f50346e6c5966475a66564f0a697943742f4f355
0112	87a506b793374513d0a3d766437730a2d2d2d2d2d454e44205047502050524956415
0113	445204b455920424c4f434b2d2d2d2d2d0a"/>
0114	</KeyValue>
0115	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0116	<CryptographicLength type="Integer" value="2048"/>
0117	</KeyBlock>
0118	</PGPKey>
0119	</RequestPayload>
0120	</BatchItem>
0121	</RequestMessage>
0122	<ResponseMessage>
0123	<ResponseHeader>
0124	<ProtocolVersion>
0125	<ProtocolVersionMajor type="Integer" value="1"/>
0126	<ProtocolVersionMinor type="Integer" value="2"/>
0127	</ProtocolVersion>
0128	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0129	<BatchCount type="Integer" value="1"/>
0130	</ResponseHeader>
0131	<BatchItem>
0132	<Operation type="Enumeration" value="Register"/>
0133	<ResultStatus type="Enumeration" value="Success"/>
0134	<ResponsePayload>
0135	<UniqueIdentifier type="TextString"
0136	value="\$UNIQUE_IDENTIFIER_1"/>
0137	</ResponsePayload>
0138	</BatchItem>
0139	</ResponseMessage>
0140	# TIME 2
0141	<RequestMessage>
0142	<RequestHeader>
0143	<ProtocolVersion>
0144	<ProtocolVersionMajor type="Integer" value="1"/>
0145	<ProtocolVersionMinor type="Integer" value="2"/>
0146	</ProtocolVersion>
0147	<BatchCount type="Integer" value="1"/>
0148	</RequestHeader>
0149	<BatchItem>
0150	<Operation type="Enumeration" value="AddAttribute"/>
0151	<UniqueBatchItemID type="ByteString" value="31f81bfb0f0492bd"/>
0152	<RequestPayload>
0153	<UniqueIdentifier type="TextString"
0154	value="\$UNIQUE_IDENTIFIER_0"/>
0155	<Attribute>
0156	<AttributeName type="TextString" value="Link"/>
0157	<AttributeValue>
0158	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0159	<LinkedObjectIdentifier type="TextString"
0160	value="\$UNIQUE_IDENTIFIER_1"/>
0161	</AttributeValue>
0162	</Attribute>
0163	</RequestPayload>
0164	</BatchItem>
0165	</RequestMessage><ResponseMessage>

0157	<ResponseHeader>
0158	<ProtocolVersion>
0159	<ProtocolVersionMajor type="Integer" value="1"/>
0160	<ProtocolVersionMinor type="Integer" value="2"/>
0161	</ProtocolVersion>
0162	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0163	<BatchCount type="Integer" value="1"/>
0164	</ResponseHeader>
0165	<BatchItem>
0166	<Operation type="Enumeration" value="AddAttribute"/>
0167	<UniqueBatchItemID type="ByteString" value="31f81bfb0f0492bd"/>
0168	<ResultStatus type="Enumeration" value="Success"/>
0169	<ResponsePayload>
0170	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0171	<Attribute>
0172	<AttributeName type="TextString" value="Link"/>
0173	<AttributeValue>
0174	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0175	<LinkedObjectIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0176	</AttributeValue>
0177	</Attribute>
0178	</ResponsePayload>
0179	</BatchItem>
0180	</ResponseMessage>
0181	<RequestMessage>
0182	<RequestHeader>
0183	<ProtocolVersion>
0184	<ProtocolVersionMajor type="Integer" value="1"/>
0185	<ProtocolVersionMinor type="Integer" value="2"/>
0186	</ProtocolVersion>
0187	<BatchCount type="Integer" value="1"/>
0188	</RequestHeader>
0189	<BatchItem>
0190	<Operation type="Enumeration" value="GetAttributeList"/>
0191	<RequestPayload>
0192	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0193	</RequestPayload>
0194	</BatchItem>
0195	</RequestMessage>
	# TIME 3
0196	<ResponseMessage>
0197	<ResponseHeader>
0198	<ProtocolVersion>
0199	<ProtocolVersionMajor type="Integer" value="1"/>
0200	<ProtocolVersionMinor type="Integer" value="2"/>
0201	</ProtocolVersion>
0202	<TimeStamp type="DateTime" value="2012-04-27T08:14:36+00:00"/>
0203	<BatchCount type="Integer" value="1"/>
0204	</ResponseHeader>
0205	<BatchItem>
0206	<Operation type="Enumeration" value="GetAttributeList"/>
0207	<ResultStatus type="Enumeration" value="Success"/>
0208	<ResponsePayload>
0209	<UniqueIdentifier type="TextString"

0210	value="\$UNIQUE_IDENTIFIER_0"/>
0211	<AttributeName type="TextString" value="x-ID"/>
0212	<AttributeName type="TextString" value="Unique Identifier"/>
0213	<AttributeName type="TextString" value="Object Type"/>
0214	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0215	<AttributeName type="TextString" value="Cryptographic Length"/>
0216	<AttributeName type="TextString" value="Digest"/>
0217	<AttributeName type="TextString" value="Initial Date"/>
0218	<AttributeName type="TextString" value="Last Change Date"/>
0219	<AttributeName type="TextString" value="Lease Time"/>
0220	<AttributeName type="TextString" value="Link"/>
0221	<AttributeName type="TextString" value="State"/>
0222	<AttributeName type="TextString" value="Alternative Name"/>
0223	</ResponsePayload>
0224	</BatchItem>
0225	</ResponseMessage>
0226	<RequestMessage>
0227	<RequestHeader>
0228	<ProtocolVersion>
0229	<ProtocolVersionMajor type="Integer" value="1"/>
0230	<ProtocolVersionMinor type="Integer" value="2"/>
0231	</ProtocolVersion>
0232	<BatchCount type="Integer" value="1"/>
0233	</RequestHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="GetAttributes"/>
0236	<RequestPayload>
0237	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0238	<AttributeName type="TextString" value="Alternative Name"/>
0239	</RequestPayload>
0240	</BatchItem>
0241	</RequestMessage>
0242	# TIME 4
0243	<ResponseMessage>
0244	<ResponseHeader>
0245	<ProtocolVersion>
0246	<ProtocolVersionMajor type="Integer" value="1"/>
0247	<ProtocolVersionMinor type="Integer" value="2"/>
0248	</ProtocolVersion>
0249	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0250	<BatchCount type="Integer" value="1"/>
0251	</ResponseHeader>
0252	<BatchItem>
0253	<Operation type="Enumeration" value="GetAttributes"/>
0254	<ResultStatus type="Enumeration" value="Success"/>
0255	<ResponsePayload>
0256	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0257	<Attribute>
0258	<AttributeName type="TextString" value="Alternative Name"/>
0259	<AttributeValue>
	<AlternativeNameValue type="TextString" value="kmip3@kmip.com"/>
	<AlternativeNameType type="Enumeration"

0260	value="UninterpretedTextString"/>
0261	</AttributeValue>
0262	</Attribute>
0263	<Attribute type="TextString" value="Alternative Name"/>
0264	<AttributeIndex type="Integer" value="1"/>
0265	<AttributeValue>
0266	<AlternativeNameValue type="TextString" value="KMIP USER RSA (OASIS Key Management Interoperability Protocol) <kmip3@kmip.com>"/>
0267	<AlternativeNameType type="Enumeration"
0268	value="UninterpretedTextString"/>
0269	</AttributeValue>
0270	</Attribute>
0271	<Attribute type="TextString" value="Alternative Name"/>
0272	<AttributeIndex type="Integer" value="2"/>
0273	<AttributeValue>
0274	<AlternativeNameValue type="TextString" value="6CCA0D26"/>
0275	<AlternativeNameType type="Enumeration"
0276	value="ObjectSerialNumber"/>
0277	</AttributeValue>
0278	</Attribute>
0279	<Attribute type="TextString" value="Alternative Name"/>
0280	<AttributeIndex type="Integer" value="3"/>
0281	<AttributeValue>
0282	<AlternativeNameValue type="TextString"
0283	value="240C17B36CCA0D26"/>
0284	<AlternativeNameType type="Enumeration"
0285	value="ObjectSerialNumber"/>
0286	</AttributeValue>
0287	</Attribute>
0288	</ResponsePayload>
0289	</BatchItem>
0290	</ResponseMessage>
0291	<RequestMessage>
0292	<RequestHeader>
0293	<ProtocolVersion>
0294	<ProtocolVersionMajor type="Integer" value="1"/>
0295	<ProtocolVersionMinor type="Integer" value="2"/>
0296	</ProtocolVersion>
0297	<BatchCount type="Integer" value="1"/>
0298	</RequestHeader>
0299	<BatchItem>
0300	<Operation type="Enumeration" value="Get"/>
0301	<RequestPayload>
0302	<UniqueIdentifier type="TextString"
0303	value="\$UNIQUE_IDENTIFIER_1"/>
0304	</RequestPayload>
0305	</BatchItem>
0306	</RequestMessage>
0307	# TIME 5
0308	<ResponseMessage>
0309	<ResponseHeader>
0310	<ProtocolVersion>
0311	<ProtocolVersionMajor type="Integer" value="1"/>

```
0308     <ProtocolVersionMinor type="Integer" value="2"/>
0309     </ProtocolVersion>
0310     <TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0311     <BatchCount type="Integer" value="1"/>
0312     </ResponseHeader>
0313     <BatchItem>
0314         <Operation type="Enumeration" value="Get"/>
0315         <ResultStatus type="Enumeration" value="Success"/>
0316         <ResponsePayload>
0317             <ObjectType type="Enumeration" value="PGPKey"/>
0318             <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0319             <PGPKey>
0320                 <PGPKeyVersion type="Integer" value="4"/>
0321                 <KeyBlock>
0322                     <KeyFormatType type="Enumeration" value="Raw"/>
0323                     <KeyValue>
0324                         <KeyMaterial type="ByteString"
value="2d2d2d2d2d424547494e205047502050524956415445204b455920424c4f4
34b2d2d2d2d0a0a6c514f2b424648412f645142434144676564396536746962386
b6c4668507077536e69314a7365636b716a534c35775431514b4b6d4a4d4d5279493
1527535520a724a53426352776a4f6f6161526461766e5a454a3178756a5533325a6
a2b3248327371733673536e697a434e6e6b46354843574f324a3362354d3576506b6
4470a505971726c6376376c7650385030776a63544f756544786e53677836496a6e3
451446a642b744c6e5478544b38553059687a73475a4377752b3353366b7768670a7
86c57537a2b33396f50306b5435382b4a766e6c7838766f777476715a2b376e70717
24d4f6f6a495665644653666b2b7a32436f31554f626a366c2b787a54740a316b715
15a6658432f79794d414677544b635045792f4b4377367532627a766f755a4d4d336
46b6766552f41757171704b5342414248305a2f626c6e433254790a516453754f4b7
87a676379494263573577526e4b746a737457395943662f6a49364574414245424
141482b41774d434b4a6258597a3633486a5a67703532300a536e5433316a574d784
c6e452b4134534e7736434f54532f36627267484a56436b50596e4f525a5144706f6
16b4a672b4638485771782b6d6f764f366c30554e0a646a3067717952344e462f327
44d76674b545430464d6472374c7269534c517343436835457771586d32766e66763
9703471664c3042746a744143762b35585a0a445a587964614674625367453862624
c652f4146514c71504f64574f746f4c43482f454430523534512b566369615a6d6f6
76941566277496a596b4e57784d560a316753455470774c3734467a6775304469674
64a7045375379687152536444736b4d586c79416d5a776730756f4c4443744e38615
97253456a724273793752740a33333741735753534d7a6e4674797a5962563150687
4486830476848426455726f2f344164356f37364d7365743342636c4d36554167365
54d53626a432f76760a55367950796a65387965707643666f762f473774535162694
94577534f585578616d6d326574766e6f3359424d786d356c3778395a50375a667a3
82b7a63564a0a6d41567853352f5151477639454d464f4747595751355a6354636b5
12b65476e7a5a4d516d42366a5657616871553869584d332f6735593849503569383
74f590a7a4c486879627032345258794f6f546942327278756c7a6d4d5655594b6c6
76436674e6c48647973514d344b316465487738523337652f4e4b4a726d47582b330
a707348494e7035454a716e42334a66513370374137434d68634a35506878336d395
56d43724b6c79474d4a6446436c2b744e32503551534138644163686776420a43304
c346f5a383343435a556d6d4d346c6a492b426f73634c4f67794b53506d73706c7a7
27a344c375472484d384b357a466f58486b5a7a5050575a544d32350a696c5479776
f67735568715865397779796177365048544842792b6331687658634851666646776
67165794b654f356e47754b425a63707173584a672f5a67310a72714b6d725532617
a64326d477459696b516d786c6b522b494f39644435384237674f416b797a4148653
54e617554393043744c3637716a4158322b614a52620a757532464c44317955424d6
a7066557133613573516c36716f392f724338696b6e44412f684642704944334c527
1444a47745961665076386f36466a5a4831550a7255437838305930726d4e656c563
63558507445382b736f32486c2f686777484552644e7370695473474553665345315
```


	27875754e532b6946572f67537933430a457252505330314a554342565530565349464a545153416f5430465453564d675332563549453168626d466e5a57316c626e5167535735305a584a76634756790a59574a7062476c3065534251636d393062324e7662436b67504774746158417a514774746158417559323974506f6b424e6751544151494149415543556344390a314149624c77594c4351674841774945465149494177515741674d42416834424168654141416f4a4543514d46374e737967306d523355482f3038756d455a760a45383762764a374a66304b646e396d784539735a55645a6559784861754a6567466348555648683256583965654374362b54684a6b466355677248624453476d0a6c4a425743734570674b617a2b455549704a78567056747731444c777652446c4d324d552f50484a51412f7777745157373547766b3469493868693459557a620a7043644d46384d5536454f4873792b4f5062425a53356c76616858714c71435033755a2f49306e57596b642b76347873377145463573412b2b657a7152694b390a49504b7361765470796c52713268364854375a6733626c643053594f545275724c32536b6b7a41654f4e517554436577574e752f347146664758614d627161550a536f3249434a5255392b31646a6a49715a4e2b49466c72676e5350546969615254776d50682b2b5751366a616a7152757a3647326f50346e6c5966475a66564f0a697943742f4f35587a506b793374513d0a3d766437730a2d2d2d2d454e44205047502050524956415445204b455920424c4f434b2d2d2d2d2d0a"/>
0325	</KeyValue>
0326	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0327	<CryptographicLength type="Integer" value="2048"/>
0328	</KeyBlock>
0329	</PGPKey>
0330	</ResponsePayload>
0331	</BatchItem>
0332	</ResponseMessage>
0333	<RequestMessage>
0334	<RequestHeader>
0335	<ProtocolVersion>
0336	<ProtocolVersionMajor type="Integer" value="1"/>
0337	<ProtocolVersionMinor type="Integer" value="2"/>
0338	</ProtocolVersion>
0339	<BatchCount type="Integer" value="1"/>
0340	</RequestHeader>
0341	<BatchItem>
0342	<Operation type="Enumeration" value="Get"/>
0343	<RequestPayload>
0344	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0345	<KeyFormatType type="Enumeration" value="Raw"/>
0346	</RequestPayload>
0347	</BatchItem>
0348	</RequestMessage>
	# TIME 6
0349	<ResponseMessage>
0350	<ResponseHeader>
0351	<ProtocolVersion>
0352	<ProtocolVersionMajor type="Integer" value="1"/>
0353	<ProtocolVersionMinor type="Integer" value="2"/>
0354	</ProtocolVersion>
0355	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0356	<BatchCount type="Integer" value="1"/>
0357	</ResponseHeader>
0358	<BatchItem>
0359	<Operation type="Enumeration" value="Get"/>
0360	<ResultStatus type="Enumeration" value="Success"/>
0361	<ResponsePayload>

0362	<ObjectType type="Enumeration" value="PGPKey"/>
0363	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0364	<PGPKey>
0365	<PGPKeyVersion type="Integer" value="4"/>
0366	<KeyBlock>
0367	<KeyFormatType type="Enumeration" value="Raw"/>
0368	<KeyValue>
0369	<KeyMaterial type="ByteString"
	value="2d2d2d2d2d424547494e20504750205055424c4943204b455920424c4f434
	b2d2d2d2d2d0a0a6d51454e424648412f645142434144676564396536746962386b6
	c4668507077536e69314a7365636b716a534c35775431514b4b6d4a4d4d527949315
	27535520a724a53426352776a4f6f6161526461766e5a454a3178756a5533325a6a2
	b3248327371733673536e697a434e6e6b46354843574f324a3362354d3576506b644
	70a505971726c6376376c7650385030776a63544f756544786e53677836496a6e345
	1446a642b744c6e5478544b38553059687a73475a4377752b3353366b7768670a786
	c57537a2b33396f50306b5435382b4a766e6c7838766f777476715a2b376e7071724
	d4f6f6a495665644653666b2b7a32436f31554f626a366c2b787a54740a316b71515
	a6658432f79794d414677544b635045792f4b4377367532627a766f755a4d4d33646
	b6766552f41757171704b5342414248305a2f626c6e433254790a516453754f4b787
	a676379494263573577526e4b746a73745757395943662f6a4936457441424542414
	147305430744e5356416756564e4655694253553045670a4b45394255306c5449457
	46c6553424e595735685a3256745a57353049456c75644756796233426c636d46696
	157787064486b6755484a766447396a623277700a4944787262576c774d304272625
	76c774c6d4e766254364a415459454577454341434146416c48412f6451434779384
	743776b4942774d434242554343414d450a4667494441514965415149586741414b4
	352416b4442657a624d6f4e4a6b6431422f39504c7068476278504f3237796579583
	9436e5a2f5a73525062475648570a586d4d52327269586f42584231465234646c562
	f586e677265766b34535a425846494b783277306870705351566772424b59436d732
	f6846434b5363566156620a634e5179384c305135544e6a46507a7879554150384d4
	c5546752b5272354f49695049597547464d3236516e54426644464f684468374d766
	a6a32775755755a0a62326f56366936676a39376d66794e4a316d4a4866722b4d624
	f36684265624150766e73366b596976534479724772303663705561746f6568302b3
	2594e32350a5864456d446b30627179396b704a4d77486a6a554c6b776e73466a627
	62b4b6858786c326a47366d6c45714e6941695556506674585934794b6d546669425
	a610a344a306a30346f6d6b55384a6a3466766c6b4f6f326f366b62732b687471442
	b4a355748786d5831546f736772667a7556387a354d7437550a3d6e564f790a2d2d2
	d2d2d454e4420504750205055424c4943204b455920424c4f434b2d2d2d2d2d0a"/>
0370	</KeyValue>
0371	<CryptographicAlgorithm type="Enumeration" value="RSA"/>
0372	<CryptographicLength type="Integer" value="2048"/>
0373	</KeyBlock>
0374	</PGPKey>
0375	</ResponsePayload>
0376	</BatchItem>
0377	</ResponseMessage>
0378	<RequestMessage>
0379	<RequestHeader>
0380	<ProtocolVersion>
0381	<ProtocolVersionMajor type="Integer" value="1"/>
0382	<ProtocolVersionMinor type="Integer" value="2"/>
0383	</ProtocolVersion>
0384	<BatchCount type="Integer" value="1"/>
0385	</RequestHeader>
0386	<BatchItem>
0387	<Operation type="Enumeration" value="Destroy"/>
0388	<RequestPayload>

0389	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0390	</RequestPayload>
0391	</BatchItem>
0392	</RequestMessage>
# TIME 7	
0393	<ResponseMessage>
0394	<ResponseHeader>
0395	<ProtocolVersion>
0396	<ProtocolVersionMajor type="Integer" value="1"/>
0397	<ProtocolVersionMinor type="Integer" value="2"/>
0398	</ProtocolVersion>
0399	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0400	<BatchCount type="Integer" value="1"/>
0401	</ResponseHeader>
0402	<BatchItem>
0403	<Operation type="Enumeration" value="Destroy"/>
0404	<ResultStatus type="Enumeration" value="Success"/>
0405	<ResponsePayload>
0406	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0407	</ResponsePayload>
0408	</BatchItem>
0409	</ResponseMessage>
0410	<RequestMessage>
0411	<RequestHeader>
0412	<ProtocolVersion>
0413	<ProtocolVersionMajor type="Integer" value="1"/>
0414	<ProtocolVersionMinor type="Integer" value="2"/>
0415	</ProtocolVersion>
0416	<BatchCount type="Integer" value="1"/>
0417	</RequestHeader>
0418	<BatchItem>
0419	<Operation type="Enumeration" value="Destroy"/>
0420	<RequestPayload>
0421	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0422	</RequestPayload>
0423	</BatchItem>
0424	</RequestMessage>
# TIME 8	
0425	<ResponseMessage>
0426	<ResponseHeader>
0427	<ProtocolVersion>
0428	<ProtocolVersionMajor type="Integer" value="1"/>
0429	<ProtocolVersionMinor type="Integer" value="2"/>
0430	</ProtocolVersion>
0431	<TimeStamp type="DateTime" value="2012-04-27T08:14:37+00:00"/>
0432	<BatchCount type="Integer" value="1"/>
0433	</ResponseHeader>
0434	<BatchItem>
0435	<Operation type="Enumeration" value="Destroy"/>
0436	<ResultStatus type="Enumeration" value="Success"/>
0437	<ResponsePayload>
0438	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0439	</ResponsePayload>
0440	</BatchItem>
0441	</ResponseMessage>

1202

1203 2.3.43 TC-MDO-1-12 - Register MDO Key

1204 Client registers a metadata-only object with the key management server and then locates and
1205 gets the value and the associated attributes. Finally the managed object is destroyed.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchOrderOption type="Boolean" value="true"/>
0008	<BatchCount type="Integer" value="1"/>
0009	</RequestHeader>
0010	<BatchItem>
0011	<Operation type="Enumeration" value="Register"/>
0012	<RequestPayload>
0013	<ObjectType type="Enumeration" value="SymmetricKey"/>
0014	<TemplateAttribute>
0015	<Attribute>
0016	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic Length"/>
0021	<AttributeValue type="Integer" value="128"/>
0022	</Attribute>
0023	<Attribute>
0024	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0025	<AttributeValue type="Integer" value="Encrypt Verify Sign"/>
0026	</Attribute>
0027	<Attribute>
0028	<AttributeName type="TextString" value="Key Value Location"/>
0029	<AttributeValue>
0030	<KeyValueLocationValue type="TextString" value="HSM- 12345"/>
0031	<KeyValueLocationType type="Enumeration" value="UninterpretedTextString"/>
0032	</AttributeValue>
0033	</Attribute>
0034	<Attribute>
0035	<AttributeName type="TextString" value="Name"/>
0036	<AttributeValue>
0037	<NameValue type="TextString" value="MDO-M-1-12"/>
0038	<NameType type="Enumeration"

0039	value="UninterpretedTextString"/>
0040	</AttributeValue>
0041	</Attribute>
0042	</TemplateAttribute>
0043	<SymmetricKey>
0044	<KeyBlock>
0045	<KeyFormatType type="Enumeration" value="Raw"/>
0046	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0047	<CryptographicLength type="Integer" value="128"/>
0048	</KeyBlock>
0049	</SymmetricKey>
0050	</RequestPayload>
0051	</BatchItem>
0052	</RequestMessage>
0053	<ResponseMessage>
0054	<ResponseHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="2"/>
0058	</ProtocolVersion>
0059	<TimeStamp type="DateTime" value="2012-11-27T23:21:22+00:00"/>
0060	<BatchCount type="Integer" value="1"/>
0061	</ResponseHeader>
0062	<BatchItem>
0063	<Operation type="Enumeration" value="Register"/>
0064	<ResultStatus type="Enumeration" value="Success"/>
0065	<ResponsePayload>
0066	<UniqueIdentifier type="TextString"
0067	value="\$UNIQUE_IDENTIFIER_0"/>
0068	</ResponsePayload>
0069	</BatchItem>
0070	</ResponseMessage>
0071	# TIME 1
0072	<RequestMessage>
0073	<RequestHeader>
0074	<ProtocolVersion>
0075	<ProtocolVersionMajor type="Integer" value="1"/>
0076	<ProtocolVersionMinor type="Integer" value="2"/>
0077	</ProtocolVersion>
0078	<BatchOrderOption type="Boolean" value="true"/>
0079	<BatchCount type="Integer" value="1"/>
0080	</RequestHeader>
0081	<BatchItem>
0082	<Operation type="Enumeration" value="Get"/>
0083	<RequestPayload>
0084	<UniqueIdentifier type="TextString"
0085	value="\$UNIQUE_IDENTIFIER_0"/>
0086	</RequestPayload>
0087	</BatchItem>
0088	</RequestMessage>
0089	<ResponseMessage>
0090	<ResponseHeader>
	<ProtocolVersion>
	<ProtocolVersionMajor type="Integer" value="1"/>
	<ProtocolVersionMinor type="Integer" value="2"/>
	</ProtocolVersion>

0091	<TimeStamp type="DateTime" value="2012-11-28T00:15:10+00:00"/>
0092	<BatchCount type="Integer" value="1"/>
0093	</ResponseHeader>
0094	<BatchItem>
0095	<Operation type="Enumeration" value="Get"/>
0096	<ResultStatus type="Enumeration" value="Success"/>
0097	<ResponsePayload>
0098	<ObjectType type="Enumeration" value="SymmetricKey"/>
0099	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0100	<SymmetricKey>
0101	<KeyBlock>
0102	<KeyFormatType type="Enumeration" value="Raw"/>
0103	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0104	<CryptographicLength type="Integer" value="128"/>
0105	</KeyBlock>
0106	</SymmetricKey>
0107	</ResponsePayload>
0108	</BatchItem>
0109	</ResponseMessage>
	# TIME 2
0110	<RequestMessage>
0111	<RequestHeader>
0112	<ProtocolVersion>
0113	<ProtocolVersionMajor type="Integer" value="1"/>
0114	<ProtocolVersionMinor type="Integer" value="2"/>
0115	</ProtocolVersion>
0116	<BatchOrderOption type="Boolean" value="true"/>
0117	<BatchCount type="Integer" value="1"/>
0118	</RequestHeader>
0119	<BatchItem>
0120	<Operation type="Enumeration" value="GetAttributes"/>
0121	<RequestPayload>
0122	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0123	<AttributeName type="TextString" value="Key Value Location"/>
0124	<AttributeName type="TextString" value="Key Value Present"/>
0125	<AttributeName type="TextString" value="Original Creation
	Date"/>
0126	</RequestPayload>
0127	</BatchItem>
0128	</RequestMessage>
0129	<ResponseMessage>
0130	<ResponseHeader>
0131	<ProtocolVersion>
0132	<ProtocolVersionMajor type="Integer" value="1"/>
0133	<ProtocolVersionMinor type="Integer" value="2"/>
0134	</ProtocolVersion>
0135	<TimeStamp type="DateTime" value="2012-11-28T00:48:54+00:00"/>
0136	<BatchCount type="Integer" value="1"/>
0137	</ResponseHeader>
0138	<BatchItem>
0139	<Operation type="Enumeration" value="GetAttributes"/>
0140	<ResultStatus type="Enumeration" value="Success"/>
0141	<ResponsePayload>
0142	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0143	<Attribute>
0144	<AttributeName type="TextString" value="Key Value Location"/>
0145	<AttributeValue>
0146	<KeyValueLocationValue type="TextString" value="HSM-12345"/>
0147	<KeyValueLocationType type="Enumeration" value="UninterpretedTextString"/>
0148	</AttributeValue>
0149	</Attribute>
0150	<Attribute>
0151	<AttributeName type="TextString" value="Key Value Present"/>
0152	<AttributeValue type="Boolean" value="false"/>
0153	</Attribute>
0154	</ResponsePayload>
0155	</BatchItem>
0156	</ResponseMessage>
# TIME 3	
0157	<RequestMessage>
0158	<RequestHeader>
0159	<ProtocolVersion>
0160	<ProtocolVersionMajor type="Integer" value="1"/>
0161	<ProtocolVersionMinor type="Integer" value="2"/>
0162	</ProtocolVersion>
0163	<BatchOrderOption type="Boolean" value="true"/>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Destroy"/>
0168	<RequestPayload>
0169	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0170	</RequestPayload>
0171	</BatchItem>
0172	</RequestMessage>
0173	<ResponseMessage>
0174	<ResponseHeader>
0175	<ProtocolVersion>
0176	<ProtocolVersionMajor type="Integer" value="1"/>
0177	<ProtocolVersionMinor type="Integer" value="2"/>
0178	</ProtocolVersion>
0179	<TimeStamp type="DateTime" value="2013-06-14T07:00:22+00:00"/>
0180	<BatchCount type="Integer" value="1"/>
0181	</ResponseHeader>
0182	<BatchItem>
0183	<Operation type="Enumeration" value="Destroy"/>
0184	<ResultStatus type="Enumeration" value="Success"/>
0185	<ResponsePayload>
0186	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0187	</ResponsePayload>
0188	</BatchItem>
0189	</ResponseMessage>

1206

1207 2.3.44 TC-MDO-2-12 - Locate MDO keys by Key Value Present

- 1208 Client registers both a metadata-only object and a normal object with key management server
1209 and then locates just the metadata-only object, and gets the value and the associated attributes.
1210 Finally the managed object is destroyed.

```
# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="2"/>
0006     </ProtocolVersion>
0007     <BatchOrderOption type="Boolean" value="true"/>
0008     <BatchCount type="Integer" value="1"/>
0009   </RequestHeader>
0010   <BatchItem>
0011     <Operation type="Enumeration" value="Register"/>
0012     <RequestPayload>
0013       <ObjectType type="Enumeration" value="SymmetricKey"/>
0014       <TemplateAttribute>
0015         <Attribute>
0016           <AttributeName type="TextString" value="Cryptographic
0017 Algorithm"/>
0018           <AttributeValue type="Enumeration" value="AES"/>
0019         </Attribute>
0020         <Attribute>
0021           <AttributeName type="TextString" value="Cryptographic
0022 Length"/>
0023           <AttributeValue type="Integer" value="128"/>
0024         </Attribute>
0025         <Attribute>
0026           <AttributeName type="TextString" value="Cryptographic
0027 Usage Mask"/>
0028           <AttributeValue type="Integer" value="Encrypt Verify
0029 Sign"/>
0030         </Attribute>
0031         <Attribute>
0032           <AttributeName type="TextString" value="Key Value
0033 Location"/>
0034           <AttributeValue>
0035             <KeyValueLocationValue type="TextString" value="HSM-
0036 12345"/>
0037             <KeyValueLocationType type="Enumeration"
0038 value="UninterpretedTextString"/>
0039           </AttributeValue>
0040         </Attribute>
0041         <Attribute>
0042           <AttributeName type="TextString" value="Name"/>
0043           <AttributeValue>
0044             <NameValue type="TextString" value="MDO-M-2-12-mdokey"/>
0045             <NameType type="Enumeration"
0046 value="UninterpretedTextString"/>
0047           </AttributeValue>
0048         </Attribute>
0049       </TemplateAttribute>
0050     </RequestPayload>
0051   </BatchItem>
0052 </BatchItem>
0053 </RequestMessage>
```


0042	<SymmetricKey>
0043	<KeyBlock>
0044	<KeyFormatType type="Enumeration" value="Raw"/>
0045	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0046	<CryptographicLength type="Integer" value="128"/>
0047	</KeyBlock>
0048	</SymmetricKey>
0049	</RequestPayload>
0050	</BatchItem>
0051	</RequestMessage>
0052	<ResponseMessage>
0053	<ResponseHeader>
0054	<ProtocolVersion>
0055	<ProtocolVersionMajor type="Integer" value="1"/>
0056	<ProtocolVersionMinor type="Integer" value="2"/>
0057	</ProtocolVersion>
0058	<TimeStamp type="DateTime" value="2012-11-27T23:21:22+00:00"/>
0059	<BatchCount type="Integer" value="1"/>
0060	</ResponseHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<ResultStatus type="Enumeration" value="Success"/>
0064	<ResponsePayload>
0065	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
	# TIME 1
0069	<RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="2"/>
0074	</ProtocolVersion>
0075	<BatchOrderOption type="Boolean" value="true"/>
0076	<BatchCount type="Integer" value="1"/>
0077	</RequestHeader>
0078	<BatchItem>
0079	<Operation type="Enumeration" value="Register"/>
0080	<RequestPayload>
0081	<ObjectType type="Enumeration" value="SymmetricKey"/>
0082	<TemplateAttribute>
0083	<Attribute>
0084	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0085	<AttributeValue type="Enumeration" value="AES"/>
0086	</Attribute>
0087	<Attribute>
0088	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0089	<AttributeValue type="Integer" value="128"/>
0090	</Attribute>
0091	<Attribute>
0092	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0093	<AttributeValue type="Integer" value="Encrypt Verify

0094	<code>Sign"/></code>
0095	<code></Attribute></code>
0096	<code><Attribute type="TextString" value="Name"/></code>
0097	<code><AttributeValue></code>
0098	<code><NameValue type="TextString" value="MDO-M-2-12-non-</code>
0099	<code>mdokey"/></code>
0100	<code><NameType type="Enumeration"</code>
0101	<code>value="UninterpretedTextString"/></code>
0102	<code></AttributeValue></code>
0103	<code></Attribute></code>
0104	<code><Attribute type="TextString" value="Original Creation</code>
0105	<code>Date"/></code>
0106	<code><AttributeValue type="DateTime" value="1970-01-</code>
0107	<code>01T10:42:00+00:00"/></code>
0108	<code></Attribute></code>
0109	<code></TemplateAttribute></code>
0110	<code><SymmetricKey></code>
0111	<code><KeyBlock></code>
0112	<code><KeyFormatType type="Enumeration" value="Raw"/></code>
0113	<code><KeyValue></code>
0114	<code><KeyMaterial type="ByteString"</code>
0115	<code>value="0123456789abcdef0123456789abcdef"/></code>
0116	<code></KeyValue></code>
0117	<code><CryptographicAlgorithm type="Enumeration" value="AES"/></code>
0118	<code><CryptographicLength type="Integer" value="128"/></code>
0119	<code></KeyBlock></code>
0120	<code></SymmetricKey></code>
0121	<code></RequestPayload></code>
0122	<code></BatchItem></code>
0123	<code></RequestMessage></code>
0124	<code><ResponseMessage></code>
0125	<code><ResponseHeader></code>
0126	<code><ProtocolVersion></code>
0127	<code><ProtocolVersionMajor type="Integer" value="1"/></code>
0128	<code><ProtocolVersionMinor type="Integer" value="2"/></code>
0129	<code></ProtocolVersion></code>
0130	<code><TimeStamp type="DateTime" value="2012-11-27T23:21:22+00:00"/></code>
0131	<code><BatchCount type="Integer" value="1"/></code>
0132	<code></ResponseHeader></code>
0133	<code><BatchItem></code>
0134	<code><Operation type="Enumeration" value="Register"/></code>
0135	<code><ResultStatus type="Enumeration" value="Success"/></code>
0136	<code><ResponsePayload></code>
0137	<code><UniqueIdentifier type="TextString"</code>
0138	<code>value="\$UNIQUE_IDENTIFIER_1"/></code>
0139	<code></ResponsePayload></code>
0140	<code></BatchItem></code>
0141	<code></ResponseMessage></code>
0142	<code># TIME 2</code>
0137	<code><RequestMessage></code>
0138	<code><RequestHeader></code>
0139	<code><ProtocolVersion></code>
0140	<code><ProtocolVersionMajor type="Integer" value="1"/></code>
0141	<code><ProtocolVersionMinor type="Integer" value="2"/></code>
0142	<code></ProtocolVersion></code>

0143	<BatchOrderOption type="Boolean" value="true"/>
0144	<BatchCount type="Integer" value="1"/>
0145	</RequestHeader>
0146	<BatchItem>
0147	<Operation type="Enumeration" value="Locate"/>
0148	<RequestPayload>
0149	<Attribute>
0150	<AttributeName type="TextString" value="Key Value Present"/>
0151	<AttributeValue type="Boolean" value="false"/>
0152	</Attribute>
0153	</RequestPayload>
0154	</BatchItem>
0155	</RequestMessage>
0156	<ResponseMessage>
0157	<ResponseHeader>
0158	<ProtocolVersion>
0159	<ProtocolVersionMajor type="Integer" value="1"/>
0160	<ProtocolVersionMinor type="Integer" value="2"/>
0161	</ProtocolVersion>
0162	<TimeStamp type="DateTime" value="2013-06-14T08:35:02+00:00"/>
0163	<BatchCount type="Integer" value="1"/>
0164	</ResponseHeader>
0165	<BatchItem>
0166	<Operation type="Enumeration" value="Locate"/>
0167	<ResultStatus type="Enumeration" value="Success"/>
0168	<ResponsePayload>
0169	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0170	</ResponsePayload>
0171	</BatchItem>
0172	</ResponseMessage>
	# TIME 3
0173	<RequestMessage>
0174	<RequestHeader>
0175	<ProtocolVersion>
0176	<ProtocolVersionMajor type="Integer" value="1"/>
0177	<ProtocolVersionMinor type="Integer" value="2"/>
0178	</ProtocolVersion>
0179	<BatchOrderOption type="Boolean" value="true"/>
0180	<BatchCount type="Integer" value="1"/>
0181	</RequestHeader>
0182	<BatchItem>
0183	<Operation type="Enumeration" value="GetAttributes"/>
0184	<RequestPayload>
0185	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0186	<AttributeName type="TextString" value="Key Value Location"/>
0187	<AttributeName type="TextString" value="Key Value Present"/>
0188	<AttributeName type="TextString" value="Original Creation
	Date"/>
0189	</RequestPayload>
0190	</BatchItem>
0191	</RequestMessage>
0192	<ResponseMessage>
0193	<ResponseHeader>
0194	<ProtocolVersion>

0195	<ProtocolVersionMajor type="Integer" value="1"/>
0196	<ProtocolVersionMinor type="Integer" value="2"/>
0197	</ProtocolVersion>
0198	<TimeStamp type="DateTime" value="2012-11-28T00:48:54+00:00"/>
0199	<BatchCount type="Integer" value="1"/>
0200	</ResponseHeader>
0201	<BatchItem>
0202	<Operation type="Enumeration" value="GetAttributes"/>
0203	<ResultStatus type="Enumeration" value="Success"/>
0204	<ResponsePayload>
0205	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0206	<Attribute>
0207	<AttributeName type="TextString" value="Key Value
	Location"/>
0208	<AttributeValue>
0209	<KeyValueLocationValue type="TextString" value="HSM-
	12345"/>
0210	<KeyValueLocationType type="Enumeration"
	value="UninterpretedTextString"/>
0211	</AttributeValue>
0212	</Attribute>
0213	<Attribute>
0214	<AttributeName type="TextString" value="Key Value Present"/>
0215	<AttributeValue type="Boolean" value="false"/>
0216	</Attribute>
0217	</ResponsePayload>
0218	</BatchItem>
0219	</ResponseMessage>
	# TIME 4
0220	<RequestMessage>
0221	<RequestHeader>
0222	<ProtocolVersion>
0223	<ProtocolVersionMajor type="Integer" value="1"/>
0224	<ProtocolVersionMinor type="Integer" value="2"/>
0225	</ProtocolVersion>
0226	<BatchOrderOption type="Boolean" value="true"/>
0227	<BatchCount type="Integer" value="1"/>
0228	</RequestHeader>
0229	<BatchItem>
0230	<Operation type="Enumeration" value="GetAttributes"/>
0231	<RequestPayload>
0232	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0233	<AttributeName type="TextString" value="Key Value Location"/>
0234	<AttributeName type="TextString" value="Key Value Present"/>
0235	<AttributeName type="TextString" value="Original Creation
	Date"/>
0236	</RequestPayload>
0237	</BatchItem>
0238	</RequestMessage>
0239	<ResponseMessage>
0240	<ResponseHeader>
0241	<ProtocolVersion>
0242	<ProtocolVersionMajor type="Integer" value="1"/>
0243	<ProtocolVersionMinor type="Integer" value="2"/>
0244	</ProtocolVersion>

0245	<TimeStamp type="DateTime" value="2012-11-28T00:48:54+00:00"/>
0246	<BatchCount type="Integer" value="1"/>
0247	</ResponseHeader>
0248	<BatchItem>
0249	<Operation type="Enumeration" value="GetAttributes"/>
0250	<ResultStatus type="Enumeration" value="Success"/>
0251	<ResponsePayload>
0252	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0253	<Attribute>
0254	<AttributeName type="TextString" value="Original Creation
	Date"/>
0255	<AttributeValue type="DateTime" value="1970-01-
	01T10:42:00+00:00"/>
0256	</Attribute>
0257	</ResponsePayload>
0258	</BatchItem>
0259	</ResponseMessage>
# TIME 5	
0260	<RequestMessage>
0261	<RequestHeader>
0262	<ProtocolVersion>
0263	<ProtocolVersionMajor type="Integer" value="1"/>
0264	<ProtocolVersionMinor type="Integer" value="2"/>
0265	</ProtocolVersion>
0266	<BatchOrderOption type="Boolean" value="true"/>
0267	<BatchCount type="Integer" value="1"/>
0268	</RequestHeader>
0269	<BatchItem>
0270	<Operation type="Enumeration" value="Destroy"/>
0271	<RequestPayload>
0272	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0273	</RequestPayload>
0274	</BatchItem>
0275	</RequestMessage>
0276	<ResponseMessage>
0277	<ResponseHeader>
0278	<ProtocolVersion>
0279	<ProtocolVersionMajor type="Integer" value="1"/>
0280	<ProtocolVersionMinor type="Integer" value="2"/>
0281	</ProtocolVersion>
0282	<TimeStamp type="DateTime" value="2013-06-14T07:00:22+00:00"/>
0283	<BatchCount type="Integer" value="1"/>
0284	</ResponseHeader>
0285	<BatchItem>
0286	<Operation type="Enumeration" value="Destroy"/>
0287	<ResultStatus type="Enumeration" value="Success"/>
0288	<ResponsePayload>
0289	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0290	</ResponsePayload>
0291	</BatchItem>
0292	</ResponseMessage>
# TIME 6	
0293	<RequestMessage>

0294	<RequestHeader>
0295	<ProtocolVersion>
0296	<ProtocolVersionMajor type="Integer" value="1"/>
0297	<ProtocolVersionMinor type="Integer" value="2"/>
0298	</ProtocolVersion>
0299	<BatchOrderOption type="Boolean" value="true"/>
0300	<BatchCount type="Integer" value="1"/>
0301	</RequestHeader>
0302	<BatchItem>
0303	<Operation type="Enumeration" value="Destroy"/>
0304	<RequestPayload>
0305	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0306	</RequestPayload>
0307	</BatchItem>
0308	</RequestMessage>
0309	<ResponseMessage>
0310	<ResponseHeader>
0311	<ProtocolVersion>
0312	<ProtocolVersionMajor type="Integer" value="1"/>
0313	<ProtocolVersionMinor type="Integer" value="2"/>
0314	</ProtocolVersion>
0315	<TimeStamp type="DateTime" value="2013-06-14T07:00:22+00:00"/>
0316	<BatchCount type="Integer" value="1"/>
0317	</ResponseHeader>
0318	<BatchItem>
0319	<Operation type="Enumeration" value="Destroy"/>
0320	<ResultStatus type="Enumeration" value="Success"/>
0321	<ResponsePayload>
0322	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0323	</ResponsePayload>
0324	</BatchItem>
0325	</ResponseMessage>

1211

1212 2.3.45 TC-MDO-3-12 - Register MDO Key using PKCS11 URI

1213 Client registers a metadata-only object with the key management server using the URI form of
1214 the Key Value Location and then locates and gets the value and the associated attributes. Finally
1215 the managed object is destroyed.

1216 See <http://tools.ietf.org/html/draft-pechanec-pkcs11uri-10> for more details on the PKCS11 URI
1217 format.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchOrderOption type="Boolean" value="true"/>
0008	<BatchCount type="Integer" value="1"/>
0009	</RequestHeader>

0010	<BatchItem>
0011	<Operation type="Enumeration" value="Register"/>
0012	<RequestPayload>
0013	<ObjectType type="Enumeration" value="SymmetricKey"/>
0014	<TemplateAttribute>
0015	<Attribute>
0016	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0021	<AttributeValue type="Integer" value="128"/>
0022	</Attribute>
0023	<Attribute>
0024	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0025	<AttributeValue type="Integer" value="Encrypt Verify
	Sign"/>
0026	</Attribute>
0027	<Attribute>
0028	<AttributeName type="TextString" value="Key Value
	Location"/>
0029	<AttributeValue>
0030	<KeyValueLocationValue type="TextString"
	value="pkcs11:token=My%20Token;object=MDO-M-
	3;objecttype=secretkey;id=%69%95%3e%5c%f4%bd%ec%91"/>
0031	<KeyValueLocationType type="Enumeration" value="URI"/>
0032	</AttributeValue>
0033	</Attribute>
0034	<Attribute>
0035	<AttributeName type="TextString" value="Name"/>
0036	<AttributeValue>
0037	<NameValue type="TextString" value="MDO-M-3-12"/>
0038	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0039	</AttributeValue>
0040	</Attribute>
0041	</TemplateAttribute>
0042	<SymmetricKey>
0043	<KeyBlock>
0044	<KeyFormatType type="Enumeration" value="Raw"/>
0045	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0046	<CryptographicLength type="Integer" value="128"/>
0047	</KeyBlock>
0048	</SymmetricKey>
0049	</RequestPayload>
0050	</BatchItem>
0051	</RequestMessage>
0052	<ResponseMessage>
0053	<ResponseHeader>
0054	<ProtocolVersion>
0055	<ProtocolVersionMajor type="Integer" value="1"/>
0056	<ProtocolVersionMinor type="Integer" value="2"/>
0057	</ProtocolVersion>
0058	<TimeStamp type="DateTime" value="2012-11-27T23:21:22+00:00"/>

0059	<BatchCount type="Integer" value="1"/>
0060	</ResponseHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="Register"/>
0063	<ResultStatus type="Enumeration" value="Success"/>
0064	<ResponsePayload>
0065	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
# TIME 1	
0069	<RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="2"/>
0074	</ProtocolVersion>
0075	<BatchOrderOption type="Boolean" value="true"/>
0076	<BatchCount type="Integer" value="1"/>
0077	</RequestHeader>
0078	<BatchItem>
0079	<Operation type="Enumeration" value="Get"/>
0080	<RequestPayload>
0081	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0082	</RequestPayload>
0083	</BatchItem>
0084	</RequestMessage>
0085	<ResponseMessage>
0086	<ResponseHeader>
0087	<ProtocolVersion>
0088	<ProtocolVersionMajor type="Integer" value="1"/>
0089	<ProtocolVersionMinor type="Integer" value="2"/>
0090	</ProtocolVersion>
0091	<TimeStamp type="DateTime" value="2012-11-28T00:15:10+00:00"/>
0092	<BatchCount type="Integer" value="1"/>
0093	</ResponseHeader>
0094	<BatchItem>
0095	<Operation type="Enumeration" value="Get"/>
0096	<ResultStatus type="Enumeration" value="Success"/>
0097	<ResponsePayload>
0098	<ObjectType type="Enumeration" value="SymmetricKey"/>
0099	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0100	<SymmetricKey>
0101	<KeyBlock>
0102	<KeyFormatType type="Enumeration" value="Raw"/>
0103	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0104	<CryptographicLength type="Integer" value="128"/>
0105	</KeyBlock>
0106	</SymmetricKey>
0107	</ResponsePayload>
0108	</BatchItem>
0109	</ResponseMessage>
# TIME 2	

0110	<RequestMessage>
0111	<RequestHeader>
0112	<ProtocolVersion>
0113	<ProtocolVersionMajor type="Integer" value="1"/>
0114	<ProtocolVersionMinor type="Integer" value="2"/>
0115	</ProtocolVersion>
0116	<BatchOrderOption type="Boolean" value="true"/>
0117	<BatchCount type="Integer" value="1"/>
0118	</RequestHeader>
0119	<BatchItem>
0120	<Operation type="Enumeration" value="GetAttributes"/>
0121	<RequestPayload>
0122	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0123	<AttributeName type="TextString" value="Key Value Location"/>
0124	<AttributeName type="TextString" value="Key Value Present"/>
0125	<AttributeName type="TextString" value="Original Creation
	Date"/>
0126	</RequestPayload>
0127	</BatchItem>
0128	</RequestMessage>
0129	<ResponseMessage>
0130	<ResponseHeader>
0131	<ProtocolVersion>
0132	<ProtocolVersionMajor type="Integer" value="1"/>
0133	<ProtocolVersionMinor type="Integer" value="2"/>
0134	</ProtocolVersion>
0135	<TimeStamp type="DateTime" value="2012-11-28T00:48:54+00:00"/>
0136	<BatchCount type="Integer" value="1"/>
0137	</ResponseHeader>
0138	<BatchItem>
0139	<Operation type="Enumeration" value="GetAttributes"/>
0140	<ResultStatus type="Enumeration" value="Success"/>
0141	<ResponsePayload>
0142	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0143	<Attribute>
0144	<AttributeName type="TextString" value="Key Value
	Location"/>
0145	<AttributeValue>
0146	<KeyValueLocationValue type="TextString"
	value="pkcs11:token=My%20Token;object=MDO-M-
	3;objecttype=secretkey;id=%69%95%3e%5c%f4%bd%ec%91"/>
0147	<KeyValueLocationType type="Enumeration" value="URI"/>
0148	</AttributeValue>
0149	</Attribute>
0150	<Attribute>
0151	<AttributeName type="TextString" value="Key Value Present"/>
0152	<AttributeValue type="Boolean" value="false"/>
0153	</Attribute>
0154	</ResponsePayload>
0155	</BatchItem>
0156	</ResponseMessage>
	# TIME 3
0157	<RequestMessage>
0158	<RequestHeader>
0159	<ProtocolVersion>

0160	<ProtocolVersionMajor type="Integer" value="1"/>
0161	<ProtocolVersionMinor type="Integer" value="2"/>
0162	</ProtocolVersion>
0163	<BatchOrderOption type="Boolean" value="true"/>
0164	<BatchCount type="Integer" value="1"/>
0165	</RequestHeader>
0166	<BatchItem>
0167	<Operation type="Enumeration" value="Destroy"/>
0168	<RequestPayload>
0169	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0170	</RequestPayload>
0171	</BatchItem>
0172	</RequestMessage>
0173	<ResponseMessage>
0174	<ResponseHeader>
0175	<ProtocolVersion>
0176	<ProtocolVersionMajor type="Integer" value="1"/>
0177	<ProtocolVersionMinor type="Integer" value="2"/>
0178	</ProtocolVersion>
0179	<TimeStamp type="DateTime" value="2013-06-14T07:00:22+00:00"/>
0180	<BatchCount type="Integer" value="1"/>
0181	</ResponseHeader>
0182	<BatchItem>
0183	<Operation type="Enumeration" value="Destroy"/>
0184	<ResultStatus type="Enumeration" value="Success"/>
0185	<ResponsePayload>
0186	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0187	</ResponsePayload>
0188	</BatchItem>
0189	</ResponseMessage>

1218

1219 2.3.46 TC-SJ-1-12 - Create and Split/Join

1220 Create a symmetric key and perform split and join in various combinations.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0016	<AttributeValue type="Enumeration" value="AES"/>

0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="Cryptographic Length"/>
0020	<AttributeValue type="Integer" value="128"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0024	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="TC-SJ-1-12"/>
0030	<NameType type="Enumeration" value="UninterpretedTextString"/>
0031	</AttributeValue>
0032	</Attribute>
0033	</TemplateAttribute>
0034	</RequestPayload>
0035	</BatchItem>
0036	</RequestMessage>
0037	<ResponseMessage>
0038	<ResponseHeader>
0039	<ProtocolVersion>
0040	<ProtocolVersionMajor type="Integer" value="1"/>
0041	<ProtocolVersionMinor type="Integer" value="2"/>
0042	</ProtocolVersion>
0043	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0044	<BatchCount type="Integer" value="1"/>
0045	</ResponseHeader>
0046	<BatchItem>
0047	<Operation type="Enumeration" value="Create"/>
0048	<ResultStatus type="Enumeration" value="Success"/>
0049	<ResponsePayload>
0050	<ObjectType type="Enumeration" value="SymmetricKey"/>
0051	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0052	</ResponsePayload>
0053	</BatchItem>
0054	</ResponseMessage>
	# TIME 1
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="2"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="CreateSplitKey"/>
0065	<RequestPayload>
0066	<ObjectType type="Enumeration" value="SplitKey"/>
0067	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>

0068	<SplitKeyParts type="Integer" value="5"/>
0069	<SplitKeyThreshold type="Integer" value="3"/>
0070	<SplitKeyMethod type="Enumeration"
	value="PolynomialSharingGF2_8"/>
0071	<TemplateAttribute>
0072	</TemplateAttribute>
0073	</RequestPayload>
0074	</BatchItem>
0075	</RequestMessage>
0076	<ResponseMessage>
0077	<ResponseHeader>
0078	<ProtocolVersion>
0079	<ProtocolVersionMajor type="Integer" value="1"/>
0080	<ProtocolVersionMinor type="Integer" value="2"/>
0081	</ProtocolVersion>
0082	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0083	<BatchCount type="Integer" value="1"/>
0084	</ResponseHeader>
0085	<BatchItem>
0086	<Operation type="Enumeration" value="CreateSplitKey"/>
0087	<ResultStatus type="Enumeration" value="Success"/>
0088	<ResponsePayload>
0089	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0090	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0091	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0092	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0093	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_5"/>
0094	</ResponsePayload>
0095	</BatchItem>
0096	</ResponseMessage>
	# TIME 2
	# Successful Join with 3 of the required 3-of-5 keys
0097	<RequestMessage>
0098	<RequestHeader>
0099	<ProtocolVersion>
0100	<ProtocolVersionMajor type="Integer" value="1"/>
0101	<ProtocolVersionMinor type="Integer" value="2"/>
0102	</ProtocolVersion>
0103	<BatchCount type="Integer" value="1"/>
0104	</RequestHeader>
0105	<BatchItem>
0106	<Operation type="Enumeration" value="JoinSplitKey"/>
0107	<RequestPayload>
0108	<ObjectType type="Enumeration" value="SymmetricKey"/>
0109	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0110	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0111	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_5"/>
0112	<TemplateAttribute>
0113	<Attribute>

0114	<AttributeName type="TextString" value="Cryptographic
0115	Algorithm"/>
0116	<AttributeValue type="Enumeration" value="AES"/>
0117	</Attribute>
0118	<AttributeName type="TextString" value="Cryptographic
0119	Length"/>
0120	<AttributeValue type="Integer" value="128"/>
0121	</Attribute>
0122	<AttributeName type="TextString" value="Cryptographic
0123	Usage Mask"/>
0124	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0125	</Attribute>
0126	<AttributeName type="TextString" value="Name"/>
0127	<AttributeValue>
0128	<NameValue type="TextString" value="TC-SJ-1-12-join1"/>
0129	<NameType type="Enumeration"
0130	value="UninterpretedTextString"/>
0131	</AttributeValue>
0132	</Attribute>
0133	</TemplateAttribute>
0134	</RequestPayload>
0135	</BatchItem>
0136	</RequestMessage>
0137	<ResponseMessage>
0138	<ResponseHeader>
0139	<ProtocolVersion>
0140	<ProtocolVersionMajor type="Integer" value="1"/>
0141	<ProtocolVersionMinor type="Integer" value="2"/>
0142	</ProtocolVersion>
0143	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0144	<BatchCount type="Integer" value="1"/>
0145	</ResponseHeader>
0146	<BatchItem>
0147	<Operation type="Enumeration" value="JoinSplitKey"/>
0148	<ResultStatus type="Enumeration" value="Success"/>
0149	<ResponsePayload>
0150	<UniqueIdentifier type="TextString"
0151	value="\$UNIQUE_IDENTIFIER_6"/>
0152	</ResponsePayload>
0153	</BatchItem>
0154	</ResponseMessage>
0155	# TIME 3
0156	# Non-successful Join with only 2 of the required 3-of-5 keys
0157	<RequestMessage>
0158	<RequestHeader>
0159	<ProtocolVersion>
0160	<ProtocolVersionMajor type="Integer" value="1"/>
0161	<ProtocolVersionMinor type="Integer" value="2"/>
0162	</ProtocolVersion>
0163	<BatchCount type="Integer" value="1"/>
	</RequestHeader>
	<BatchItem>
	<Operation type="Enumeration" value="JoinSplitKey"/>
	<RequestPayload>

0164	<ObjectType type="Enumeration" value="SymmetricKey"/>
0165	<UniqueIdentifier type="TextString"
0166	value="\$UNIQUE_IDENTIFIER_2"/>
0167	<UniqueIdentifier type="TextString"
0168	value="\$UNIQUE_IDENTIFIER_4"/>
0169	<TemplateAttribute>
0170	<Attribute>
0171	<AttributeName type="TextString" value="Cryptographic"
0172	Algorithm"/>
0173	<AttributeValue type="Enumeration" value="AES"/>
0174	</Attribute>
0175	<Attribute>
0176	<AttributeName type="TextString" value="Cryptographic"
0177	Length"/>
0178	<AttributeValue type="Integer" value="128"/>
0179	</Attribute>
0180	<Attribute>
0181	<AttributeName type="TextString" value="Cryptographic"
0182	Usage Mask"/>
0183	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0184	</Attribute>
0185	<Attribute>
0186	<AttributeName type="TextString" value="Name"/>
0187	<AttributeValue>
0188	<NameValue type="TextString" value="TC-SJ-1-12-join2"/>
0189	<NameType type="Enumeration"
0190	value="UninterpretedTextString"/>
0191	</AttributeValue>
0192	</Attribute>
0193	</TemplateAttribute>
0194	</RequestPayload>
0195	</BatchItem>
0196	</RequestMessage>
0197	<ResponseMessage>
0198	<ResponseHeader>
0199	<ProtocolVersion>
0200	<ProtocolVersionMajor type="Integer" value="1"/>
0201	<ProtocolVersionMinor type="Integer" value="2"/>
0202	</ProtocolVersion>
0203	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0204	<BatchCount type="Integer" value="1"/>
0205	</ResponseHeader>
0206	<BatchItem>
0207	<Operation type="Enumeration" value="JoinSplitKey"/>
0208	<ResultStatus type="Enumeration" value="OperationFailed"/>
0209	<ResultReason type="Enumeration" value="CryptographicFailure"/>
0210	<ResultMessage type="TextString" value="FAILURE"/>
0211	</BatchItem>
0212	</ResponseMessage>
0213	# TIME 4
0214	<RequestMessage>
0215	<RequestHeader>
0216	<ProtocolVersion>
0217	<ProtocolVersionMajor type="Integer" value="1"/>
0218	<ProtocolVersionMinor type="Integer" value="2"/>
0219	</ProtocolVersion>
0220	<BatchCount type="Integer" value="1"/>

0214	</RequestHeader>
0215	<BatchItem>
0216	<Operation type="Enumeration" value="Destroy"/>
0217	<RequestPayload>
0218	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0219	</RequestPayload>
0220	</BatchItem>
0221	</RequestMessage>
0222	<ResponseMessage>
0223	<ResponseHeader>
0224	<ProtocolVersion>
0225	<ProtocolVersionMajor type="Integer" value="1"/>
0226	<ProtocolVersionMinor type="Integer" value="2"/>
0227	</ProtocolVersion>
0228	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0229	<BatchCount type="Integer" value="1"/>
0230	</ResponseHeader>
0231	<BatchItem>
0232	<Operation type="Enumeration" value="Destroy"/>
0233	<ResultStatus type="Enumeration" value="Success"/>
0234	<ResponsePayload>
0235	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0236	</ResponsePayload>
0237	</BatchItem>
0238	</ResponseMessage>
	# TIME 5
0239	<RequestMessage>
0240	<RequestHeader>
0241	<ProtocolVersion>
0242	<ProtocolVersionMajor type="Integer" value="1"/>
0243	<ProtocolVersionMinor type="Integer" value="2"/>
0244	</ProtocolVersion>
0245	<BatchCount type="Integer" value="1"/>
0246	</RequestHeader>
0247	<BatchItem>
0248	<Operation type="Enumeration" value="Destroy"/>
0249	<RequestPayload>
0250	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0251	</RequestPayload>
0252	</BatchItem>
0253	</RequestMessage>
0254	<ResponseMessage>
0255	<ResponseHeader>
0256	<ProtocolVersion>
0257	<ProtocolVersionMajor type="Integer" value="1"/>
0258	<ProtocolVersionMinor type="Integer" value="2"/>
0259	</ProtocolVersion>
0260	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0261	<BatchCount type="Integer" value="1"/>
0262	</ResponseHeader>
0263	<BatchItem>
0264	<Operation type="Enumeration" value="Destroy"/>
0265	<ResultStatus type="Enumeration" value="Success"/>

0266	<ResponsePayload>
0267	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0268	</ResponsePayload>
0269	</BatchItem>
0270	</ResponseMessage>
# TIME 6	
0271	<RequestMessage>
0272	<RequestHeader>
0273	<ProtocolVersion>
0274	<ProtocolVersionMajor type="Integer" value="1"/>
0275	<ProtocolVersionMinor type="Integer" value="2"/>
0276	</ProtocolVersion>
0277	<BatchCount type="Integer" value="1"/>
0278	</RequestHeader>
0279	<BatchItem>
0280	<Operation type="Enumeration" value="Destroy"/>
0281	<RequestPayload>
0282	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0283	</RequestPayload>
0284	</BatchItem>
0285	</RequestMessage>
0286	<ResponseMessage>
0287	<ResponseHeader>
0288	<ProtocolVersion>
0289	<ProtocolVersionMajor type="Integer" value="1"/>
0290	<ProtocolVersionMinor type="Integer" value="2"/>
0291	</ProtocolVersion>
0292	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0293	<BatchCount type="Integer" value="1"/>
0294	</ResponseHeader>
0295	<BatchItem>
0296	<Operation type="Enumeration" value="Destroy"/>
0297	<ResultStatus type="Enumeration" value="Success"/>
0298	<ResponsePayload>
0299	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0300	</ResponsePayload>
0301	</BatchItem>
0302	</ResponseMessage>
# TIME 7	
0303	<RequestMessage>
0304	<RequestHeader>
0305	<ProtocolVersion>
0306	<ProtocolVersionMajor type="Integer" value="1"/>
0307	<ProtocolVersionMinor type="Integer" value="2"/>
0308	</ProtocolVersion>
0309	<BatchCount type="Integer" value="1"/>
0310	</RequestHeader>
0311	<BatchItem>
0312	<Operation type="Enumeration" value="Destroy"/>
0313	<RequestPayload>
0314	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0315	</RequestPayload>

0316	</BatchItem>
0317	</RequestMessage>
0318	<ResponseMessage>
0319	<ResponseHeader>
0320	<ProtocolVersion>
0321	<ProtocolVersionMajor type="Integer" value="1"/>
0322	<ProtocolVersionMinor type="Integer" value="2"/>
0323	</ProtocolVersion>
0324	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0325	<BatchCount type="Integer" value="1"/>
0326	</ResponseHeader>
0327	<BatchItem>
0328	<Operation type="Enumeration" value="Destroy"/>
0329	<ResultStatus type="Enumeration" value="Success"/>
0330	<ResponsePayload>
0331	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0332	</ResponsePayload>
0333	</BatchItem>
0334	</ResponseMessage>
	# TIME 8
0335	<RequestMessage>
0336	<RequestHeader>
0337	<ProtocolVersion>
0338	<ProtocolVersionMajor type="Integer" value="1"/>
0339	<ProtocolVersionMinor type="Integer" value="2"/>
0340	</ProtocolVersion>
0341	<BatchCount type="Integer" value="1"/>
0342	</RequestHeader>
0343	<BatchItem>
0344	<Operation type="Enumeration" value="Destroy"/>
0345	<RequestPayload>
0346	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0347	</RequestPayload>
0348	</BatchItem>
0349	</RequestMessage>
0350	<ResponseMessage>
0351	<ResponseHeader>
0352	<ProtocolVersion>
0353	<ProtocolVersionMajor type="Integer" value="1"/>
0354	<ProtocolVersionMinor type="Integer" value="2"/>
0355	</ProtocolVersion>
0356	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0357	<BatchCount type="Integer" value="1"/>
0358	</ResponseHeader>
0359	<BatchItem>
0360	<Operation type="Enumeration" value="Destroy"/>
0361	<ResultStatus type="Enumeration" value="Success"/>
0362	<ResponsePayload>
0363	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0364	</ResponsePayload>
0365	</BatchItem>
0366	</ResponseMessage>
	# TIME 9

0367	<RequestMessage>
0368	<RequestHeader>
0369	<ProtocolVersion>
0370	<ProtocolVersionMajor type="Integer" value="1"/>
0371	<ProtocolVersionMinor type="Integer" value="2"/>
0372	</ProtocolVersion>
0373	<BatchCount type="Integer" value="1"/>
0374	</RequestHeader>
0375	<BatchItem>
0376	<Operation type="Enumeration" value="Destroy"/>
0377	<RequestPayload>
0378	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_5"/>
0379	</RequestPayload>
0380	</BatchItem>
0381	</RequestMessage>
0382	<ResponseMessage>
0383	<ResponseHeader>
0384	<ProtocolVersion>
0385	<ProtocolVersionMajor type="Integer" value="1"/>
0386	<ProtocolVersionMinor type="Integer" value="2"/>
0387	</ProtocolVersion>
0388	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0389	<BatchCount type="Integer" value="1"/>
0390	</ResponseHeader>
0391	<BatchItem>
0392	<Operation type="Enumeration" value="Destroy"/>
0393	<ResultStatus type="Enumeration" value="Success"/>
0394	<ResponsePayload>
0395	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_5"/>
0396	</ResponsePayload>
0397	</BatchItem>
0398	</ResponseMessage>
	# TIME 10
0399	<RequestMessage>
0400	<RequestHeader>
0401	<ProtocolVersion>
0402	<ProtocolVersionMajor type="Integer" value="1"/>
0403	<ProtocolVersionMinor type="Integer" value="2"/>
0404	</ProtocolVersion>
0405	<BatchCount type="Integer" value="1"/>
0406	</RequestHeader>
0407	<BatchItem>
0408	<Operation type="Enumeration" value="Destroy"/>
0409	<RequestPayload>
0410	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_6"/>
0411	</RequestPayload>
0412	</BatchItem>
0413	</RequestMessage>
0414	<ResponseMessage>
0415	<ResponseHeader>
0416	<ProtocolVersion>
0417	<ProtocolVersionMajor type="Integer" value="1"/>
0418	<ProtocolVersionMinor type="Integer" value="2"/>

```

0419     </ProtocolVersion>
0420     <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0421     <BatchCount type="Integer" value="1"/>
0422 </ResponseHeader>
0423 <BatchItem>
0424     <Operation type="Enumeration" value="Destroy"/>
0425     <ResultStatus type="Enumeration" value="Success"/>
0426     <ResponsePayload>
0427         <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_6"/>
0428     </ResponsePayload>
0429 </BatchItem>
0430 </ResponseMessage>

```

1221

1222 2.3.47 TC-SJ-2-12 - Register and Split / Join

1223 Register a symmetric key and perform split and join in various combinations.

```

# TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="2"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="Register"/>
0011     <RequestPayload>
0012       <ObjectType type="Enumeration" value="SymmetricKey"/>
0013       <TemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0016           <AttributeValue type="Integer" value="Encrypt Decrypt"/>
0017         </Attribute>
0018         <Attribute>
0019           <AttributeName type="TextString" value="x-ID"/>
0020           <AttributeValue type="TextString" value="TC-SJ-2-12"/>
0021         </Attribute>
0022       </TemplateAttribute>
0023       <SymmetricKey>
0024         <KeyBlock>
0025           <KeyFormatType type="Enumeration" value="Raw"/>
0026           <KeyValue>
0027             <KeyMaterial type="ByteString"
value="0102030405060708090A0B0C0D0E0F10"/>
0028           </KeyValue>
0029           <CryptographicAlgorithm type="Enumeration" value="AES"/>
0030           <CryptographicLength type="Integer" value="128"/>
0031         </KeyBlock>
0032       </SymmetricKey>
0033     </RequestPayload>
0034   </BatchItem>

```

0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="2"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
# TIME 1	
0053	<RequestMessage>
0054	<RequestHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="2"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="CreateSplitKey"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="SplitKey"/>
0065	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0066	<SplitKeyParts type="Integer" value="4"/>
0067	<SplitKeyThreshold type="Integer" value="2"/>
0068	<SplitKeyMethod type="Enumeration"
	value="PolynomialSharingGF2_8"/>
0069	<TemplateAttribute>
0070	</TemplateAttribute>
0071	</RequestPayload>
0072	</BatchItem>
0073	</RequestMessage>
0074	<ResponseMessage>
0075	<ResponseHeader>
0076	<ProtocolVersion>
0077	<ProtocolVersionMajor type="Integer" value="1"/>
0078	<ProtocolVersionMinor type="Integer" value="2"/>
0079	</ProtocolVersion>
0080	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0081	<BatchCount type="Integer" value="1"/>
0082	</ResponseHeader>
0083	<BatchItem>
0084	<Operation type="Enumeration" value="CreateSplitKey"/>
0085	<ResultStatus type="Enumeration" value="Success"/>
0086	<ResponsePayload>

0087	<UniqueIdentifier type="TextString"
0088	value="\$UNIQUE_IDENTIFIER_1"/>
0089	<UniqueIdentifier type="TextString"
0090	value="\$UNIQUE_IDENTIFIER_2"/>
0091	<UniqueIdentifier type="TextString"
0092	value="\$UNIQUE_IDENTIFIER_3"/>
0093	<UniqueIdentifier type="TextString"
0094	value="\$UNIQUE_IDENTIFIER_4"/>
0095	</ResponsePayload>
0096	</BatchItem>
0097	</ResponseMessage>
0098	# TIME 2
0099	<RequestMessage>
0100	<RequestHeader>
0101	<ProtocolVersion>
0102	<ProtocolVersionMajor type="Integer" value="1"/>
0103	<ProtocolVersionMinor type="Integer" value="2"/>
0104	</ProtocolVersion>
0105	<BatchCount type="Integer" value="1"/>
0106	</RequestHeader>
0107	<BatchItem>
0108	<Operation type="Enumeration" value="Get"/>
0109	<RequestPayload>
0110	<UniqueIdentifier type="TextString"
0111	value="\$UNIQUE_IDENTIFIER_1"/>
0112	</RequestPayload>
0113	</BatchItem>
0114	</RequestMessage>
0115	<ResponseMessage>
0116	<ResponseHeader>
0117	<ProtocolVersion>
0118	<ProtocolVersionMajor type="Integer" value="1"/>
0119	<ProtocolVersionMinor type="Integer" value="2"/>
0120	</ProtocolVersion>
0121	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0122	<BatchCount type="Integer" value="1"/>
0123	</ResponseHeader>
0124	<BatchItem>
0125	<Operation type="Enumeration" value="Get"/>
0126	<ResultStatus type="Enumeration" value="Success"/>
0127	<ResponsePayload>
0128	<ObjectType type="Enumeration" value="SplitKey"/>
0129	<UniqueIdentifier type="TextString"
0130	value="\$UNIQUE_IDENTIFIER_1"/>
0131	<SplitKey>
0132	<SplitKeyParts type="Integer" value="4"/>
0133	<KeyPartIdentifier type="Integer" value="1"/>
0134	<SplitKeyThreshold type="Integer" value="2"/>
0135	<SplitKeyMethod type="Enumeration"
	value="PolynomialSharingGF2_8"/>
	<KeyBlock>
	<KeyFormatType type="Enumeration" value="Raw"/>
	<KeyValue>
	<KeyMaterial type="ByteString"
	value="66C46A7754F94DE420C7B1A7FFF5EC56"/>
	</KeyValue>
	<CryptographicAlgorithm type="Enumeration" value="AES"/>

0136	<CryptographicLength type="Integer" value="128"/>
0137	</KeyBlock>
0138	</SplitKey>
0139	</ResponsePayload>
0140	</BatchItem>
	</ResponseMessage>
0141	# TIME 3
0141	<RequestMessage>
0142	<RequestHeader>
0143	<ProtocolVersion>
0144	<ProtocolVersionMajor type="Integer" value="1"/>
0145	<ProtocolVersionMinor type="Integer" value="2"/>
0146	</ProtocolVersion>
0147	<BatchCount type="Integer" value="1"/>
0148	</RequestHeader>
0149	<BatchItem>
0150	<Operation type="Enumeration" value="Get"/>
0151	<RequestPayload>
0152	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0153	</RequestPayload>
0154	</BatchItem>
0155	</RequestMessage>
0156	<ResponseMessage>
0157	<ResponseHeader>
0158	<ProtocolVersion>
0159	<ProtocolVersionMajor type="Integer" value="1"/>
0160	<ProtocolVersionMinor type="Integer" value="2"/>
0161	</ProtocolVersion>
0162	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0163	<BatchCount type="Integer" value="1"/>
0164	</ResponseHeader>
0165	<BatchItem>
0166	<Operation type="Enumeration" value="Get"/>
0167	<ResultStatus type="Enumeration" value="Success"/>
0168	<ResponsePayload>
0169	<ObjectType type="Enumeration" value="SplitKey"/>
0170	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0171	<SplitKey>
0172	<SplitKeyParts type="Integer" value="4"/>
0173	<KeyPartIdentifier type="Integer" value="2"/>
0174	<SplitKeyThreshold type="Integer" value="2"/>
0175	<SplitKeyMethod type="Enumeration"
0176	value="PolynomialSharingGF2_8"/>
0177	<KeyBlock>
0178	<KeyFormatType type="Enumeration" value="Raw"/>
0179	<KeyValue>
	<KeyMaterial type="ByteString"
0180	value="CF93D1E2A7E593CD5B8D6247F4E5D49C"/>
0181	</KeyValue>
0182	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0183	<CryptographicLength type="Integer" value="128"/>
0184	</KeyBlock>
0185	</SplitKey>
0186	</ResponsePayload>
0187	</BatchItem>

	</ResponseMessage>
	# TIME 4
0188	<RequestMessage>
0189	<RequestHeader>
0190	<ProtocolVersion>
0191	<ProtocolVersionMajor type="Integer" value="1"/>
0192	<ProtocolVersionMinor type="Integer" value="2"/>
0193	</ProtocolVersion>
0194	<BatchCount type="Integer" value="1"/>
0195	</RequestHeader>
0196	<BatchItem>
0197	<Operation type="Enumeration" value="Get"/>
0198	<RequestPayload>
0199	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0200	</RequestPayload>
0201	</BatchItem>
0202	</RequestMessage>
0203	<ResponseMessage>
0204	<ResponseHeader>
0205	<ProtocolVersion>
0206	<ProtocolVersionMajor type="Integer" value="1"/>
0207	<ProtocolVersionMinor type="Integer" value="2"/>
0208	</ProtocolVersion>
0209	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0210	<BatchCount type="Integer" value="1"/>
0211	</ResponseHeader>
0212	<BatchItem>
0213	<Operation type="Enumeration" value="Get"/>
0214	<ResultStatus type="Enumeration" value="Success"/>
0215	<ResponsePayload>
0216	<ObjectType type="Enumeration" value="SplitKey"/>
0217	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0218	<SplitKey>
0219	<SplitKeyParts type="Integer" value="4"/>
0220	<KeyPartIdentifier type="Integer" value="3"/>
0221	<SplitKeyThreshold type="Integer" value="2"/>
0222	<SplitKeyMethod type="Enumeration"
0223	value="PolynomialSharingGF2_8"/>
0224	<KeyBlock>
0225	<KeyFormatType type="Enumeration" value="Raw"/>
0226	<KeyValue>
	<KeyMaterial type="ByteString"
0227	value="A855B891F61AD9217240D8EC061E37DA"/>
0228	</KeyValue>
0229	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0230	<CryptographicLength type="Integer" value="128"/>
0231	</KeyBlock>
0232	</SplitKey>
0233	</ResponsePayload>
0234	</BatchItem>
	</ResponseMessage>
	# TIME 5
0235	<RequestMessage>
0236	<RequestHeader>

0237	<ProtocolVersion>
0238	<ProtocolVersionMajor type="Integer" value="1"/>
0239	<ProtocolVersionMinor type="Integer" value="2"/>
0240	</ProtocolVersion>
0241	<BatchCount type="Integer" value="1"/>
0242	</RequestHeader>
0243	<BatchItem>
0244	<Operation type="Enumeration" value="Get"/>
0245	<RequestPayload>
0246	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0247	</RequestPayload>
0248	</BatchItem>
0249	</RequestMessage>
0250	<ResponseMessage>
0251	<ResponseHeader>
0252	<ProtocolVersion>
0253	<ProtocolVersionMajor type="Integer" value="1"/>
0254	<ProtocolVersionMinor type="Integer" value="2"/>
0255	</ProtocolVersion>
0256	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0257	<BatchCount type="Integer" value="1"/>
0258	</ResponseHeader>
0259	<BatchItem>
0260	<Operation type="Enumeration" value="Get"/>
0261	<ResultStatus type="Enumeration" value="Success"/>
0262	<ResponsePayload>
0263	<ObjectType type="Enumeration" value="SplitKey"/>
0264	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0265	<SplitKey>
0266	<SplitKeyParts type="Integer" value="4"/>
0267	<KeyPartIdentifier type="Integer" value="4"/>
0268	<SplitKeyThreshold type="Integer" value="2"/>
0269	<SplitKeyMethod type="Enumeration"
0270	value="PolynomialSharingGF2_8"/>
0271	<KeyBlock>
0272	<KeyFormatType type="Enumeration" value="Raw"/>
0273	<KeyValue>
	<KeyMaterial type="ByteString"
0274	value="803DBAD55CDD329FAD19D99AE2C5A415"/>
0275	</KeyValue>
0276	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0277	<CryptographicLength type="Integer" value="128"/>
0278	</KeyBlock>
0279	</SplitKey>
0280	</ResponsePayload>
0281	</BatchItem>
	</ResponseMessage>
	# TIME 6
	# Successful Join with 2 of the required 2-of-4 keys
0282	<RequestMessage>
0283	<RequestHeader>
0284	<ProtocolVersion>
0285	<ProtocolVersionMajor type="Integer" value="1"/>
0286	<ProtocolVersionMinor type="Integer" value="2"/>
0287	</ProtocolVersion>

0288	<BatchCount type="Integer" value="1"/>
0289	</RequestHeader>
0290	<BatchItem>
0291	<Operation type="Enumeration" value="JoinSplitKey"/>
0292	<RequestPayload>
0293	<ObjectType type="Enumeration" value="SymmetricKey"/>
0294	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0295	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0296	<TemplateAttribute>
0297	<Attribute>
0298	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0299	<AttributeValue type="Enumeration" value="AES"/>
0300	</Attribute>
0301	<Attribute>
0302	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0303	<AttributeValue type="Integer" value="128"/>
0304	</Attribute>
0305	<Attribute>
0306	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0307	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0308	</Attribute>
0309	<Attribute>
0310	<AttributeName type="TextString" value="Name"/>
0311	<AttributeValue>
0312	<NameValue type="TextString" value="TC-SJ-2-12-join1"/>
0313	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0314	</AttributeValue>
0315	</Attribute>
0316	</TemplateAttribute>
0317	</RequestPayload>
0318	</BatchItem>
0319	</RequestMessage>
0320	<ResponseMessage>
0321	<ResponseHeader>
0322	<ProtocolVersion>
0323	<ProtocolVersionMajor type="Integer" value="1"/>
0324	<ProtocolVersionMinor type="Integer" value="2"/>
0325	</ProtocolVersion>
0326	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0327	<BatchCount type="Integer" value="1"/>
0328	</ResponseHeader>
0329	<BatchItem>
0330	<Operation type="Enumeration" value="JoinSplitKey"/>
0331	<ResultStatus type="Enumeration" value="Success"/>
0332	<ResponsePayload>
0333	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_5"/>
0334	</ResponsePayload>
0335	</BatchItem>
0336	</ResponseMessage>
	# TIME 7

0337	<RequestMessage>
0338	<RequestHeader>
0339	<ProtocolVersion>
0340	<ProtocolVersionMajor type="Integer" value="1"/>
0341	<ProtocolVersionMinor type="Integer" value="2"/>
0342	</ProtocolVersion>
0343	<BatchCount type="Integer" value="1"/>
0344	</RequestHeader>
0345	<BatchItem>
0346	<Operation type="Enumeration" value="Get"/>
0347	<RequestPayload>
0348	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_5"/>
0349	</RequestPayload>
0350	</BatchItem>
0351	</RequestMessage>
0352	<ResponseMessage>
0353	<ResponseHeader>
0354	<ProtocolVersion>
0355	<ProtocolVersionMajor type="Integer" value="1"/>
0356	<ProtocolVersionMinor type="Integer" value="2"/>
0357	</ProtocolVersion>
0358	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0359	<BatchCount type="Integer" value="1"/>
0360	</ResponseHeader>
0361	<BatchItem>
0362	<Operation type="Enumeration" value="Get"/>
0363	<ResultStatus type="Enumeration" value="Success"/>
0364	<ResponsePayload>
0365	<ObjectType type="Enumeration" value="SymmetricKey"/>
0366	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_5"/>
0367	<SymmetricKey>
0368	<KeyBlock>
0369	<KeyFormatType type="Enumeration" value="Raw"/>
0370	<KeyValue>
0371	<KeyMaterial type="ByteString"
	value="0102030405060708090A0B0C0D0E0F10"/>
0372	</KeyValue>
0373	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0374	<CryptographicLength type="Integer" value="128"/>
0375	</KeyBlock>
0376	</SymmetricKey>
0377	</ResponsePayload>
0378	</BatchItem>
0379	</ResponseMessage>
	<i># TIME 8</i>
	<i># Non-successful Join with only 1 of the required 2-of-4 keys</i>
0380	<RequestMessage>
0381	<RequestHeader>
0382	<ProtocolVersion>
0383	<ProtocolVersionMajor type="Integer" value="1"/>
0384	<ProtocolVersionMinor type="Integer" value="2"/>
0385	</ProtocolVersion>
0386	<BatchCount type="Integer" value="1"/>
0387	</RequestHeader>
0388	<BatchItem>

0389	<Operation type="Enumeration" value="JoinSplitKey"/>
0390	<RequestPayload>
0391	<ObjectType type="Enumeration" value="SymmetricKey"/>
0392	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0393	</RequestPayload>
0394	</BatchItem>
0395	</RequestMessage>
0396	<ResponseMessage>
0397	<ResponseHeader>
0398	<ProtocolVersion>
0399	<ProtocolVersionMajor type="Integer" value="1"/>
0400	<ProtocolVersionMinor type="Integer" value="2"/>
0401	</ProtocolVersion>
0402	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0403	<BatchCount type="Integer" value="1"/>
0404	</ResponseHeader>
0405	<BatchItem>
0406	<Operation type="Enumeration" value="JoinSplitKey"/>
0407	<ResultStatus type="Enumeration" value="OperationFailed"/>
0408	<ResultReason type="Enumeration" value="CryptographicFailure"/>
0409	<ResultMessage type="TextString" value="FAILURE"/>
0410	</BatchItem>
0411	</ResponseMessage>
	# TIME 9
0412	<RequestMessage>
0413	<RequestHeader>
0414	<ProtocolVersion>
0415	<ProtocolVersionMajor type="Integer" value="1"/>
0416	<ProtocolVersionMinor type="Integer" value="2"/>
0417	</ProtocolVersion>
0418	<BatchCount type="Integer" value="1"/>
0419	</RequestHeader>
0420	<BatchItem>
0421	<Operation type="Enumeration" value="Destroy"/>
0422	<RequestPayload>
0423	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0424	</RequestPayload>
0425	</BatchItem>
0426	</RequestMessage>
0427	<ResponseMessage>
0428	<ResponseHeader>
0429	<ProtocolVersion>
0430	<ProtocolVersionMajor type="Integer" value="1"/>
0431	<ProtocolVersionMinor type="Integer" value="2"/>
0432	</ProtocolVersion>
0433	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0434	<BatchCount type="Integer" value="1"/>
0435	</ResponseHeader>
0436	<BatchItem>
0437	<Operation type="Enumeration" value="Destroy"/>
0438	<ResultStatus type="Enumeration" value="Success"/>
0439	<ResponsePayload>
0440	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0441	</ResponsePayload>
0442	</BatchItem>
0443	</ResponseMessage>
0444	# TIME 10
0445	<RequestMessage>
0446	<RequestHeader>
0447	<ProtocolVersion>
0448	<ProtocolVersionMajor type="Integer" value="1"/>
0449	<ProtocolVersionMinor type="Integer" value="2"/>
0450	</ProtocolVersion>
0451	<BatchCount type="Integer" value="1"/>
0452	</RequestHeader>
0453	<BatchItem>
0454	<Operation type="Enumeration" value="Destroy"/>
0455	<RequestPayload>
0456	<UniqueIdentifier type="TextString"
0457	value="\$UNIQUE_IDENTIFIER_1"/>
0458	</RequestPayload>
0459	</BatchItem>
0460	</RequestMessage>
0461	<ResponseMessage>
0462	<ResponseHeader>
0463	<ProtocolVersion>
0464	<ProtocolVersionMajor type="Integer" value="1"/>
0465	<ProtocolVersionMinor type="Integer" value="2"/>
0466	</ProtocolVersion>
0467	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0468	<BatchCount type="Integer" value="1"/>
0469	</ResponseHeader>
0470	<BatchItem>
0471	<Operation type="Enumeration" value="Destroy"/>
0472	<ResultStatus type="Enumeration" value="Success"/>
0473	<ResponsePayload>
0474	<UniqueIdentifier type="TextString"
0475	value="\$UNIQUE_IDENTIFIER_1"/>
0476	</ResponsePayload>
0477	</BatchItem>
0478	</ResponseMessage>
0479	# TIME 11
0480	<RequestMessage>
0481	<RequestHeader>
0482	<ProtocolVersion>
0483	<ProtocolVersionMajor type="Integer" value="1"/>
0484	<ProtocolVersionMinor type="Integer" value="2"/>
0485	</ProtocolVersion>
0486	<BatchCount type="Integer" value="1"/>
0487	</RequestHeader>
0488	<BatchItem>
0489	<Operation type="Enumeration" value="Destroy"/>
0490	<RequestPayload>
0491	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
	</RequestPayload>
	</BatchItem>
	</RequestMessage>
	<ResponseMessage>

0492	<ResponseHeader>
0493	<ProtocolVersion>
0494	<ProtocolVersionMajor type="Integer" value="1"/>
0495	<ProtocolVersionMinor type="Integer" value="2"/>
0496	</ProtocolVersion>
0497	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0498	<BatchCount type="Integer" value="1"/>
0499	</ResponseHeader>
0500	<BatchItem>
0501	<Operation type="Enumeration" value="Destroy"/>
0502	<ResultStatus type="Enumeration" value="Success"/>
0503	<ResponsePayload>
0504	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0505	</ResponsePayload>
0506	</BatchItem>
0507	</ResponseMessage>
# TIME 12	
0508	<RequestMessage>
0509	<RequestHeader>
0510	<ProtocolVersion>
0511	<ProtocolVersionMajor type="Integer" value="1"/>
0512	<ProtocolVersionMinor type="Integer" value="2"/>
0513	</ProtocolVersion>
0514	<BatchCount type="Integer" value="1"/>
0515	</RequestHeader>
0516	<BatchItem>
0517	<Operation type="Enumeration" value="Destroy"/>
0518	<RequestPayload>
0519	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0520	</RequestPayload>
0521	</BatchItem>
0522	</RequestMessage>
0523	<ResponseMessage>
0524	<ResponseHeader>
0525	<ProtocolVersion>
0526	<ProtocolVersionMajor type="Integer" value="1"/>
0527	<ProtocolVersionMinor type="Integer" value="2"/>
0528	</ProtocolVersion>
0529	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0530	<BatchCount type="Integer" value="1"/>
0531	</ResponseHeader>
0532	<BatchItem>
0533	<Operation type="Enumeration" value="Destroy"/>
0534	<ResultStatus type="Enumeration" value="Success"/>
0535	<ResponsePayload>
0536	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0537	</ResponsePayload>
0538	</BatchItem>
0539	</ResponseMessage>
# TIME 13	
0540	<RequestMessage>
0541	<RequestHeader>
0542	<ProtocolVersion>

0543	<ProtocolVersionMajor type="Integer" value="1"/>
0544	<ProtocolVersionMinor type="Integer" value="2"/>
0545	</ProtocolVersion>
0546	<BatchCount type="Integer" value="1"/>
0547	</RequestHeader>
0548	<BatchItem>
0549	<Operation type="Enumeration" value="Destroy"/>
0550	<RequestPayload>
0551	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0552	</RequestPayload>
0553	</BatchItem>
0554	</RequestMessage>
0555	<ResponseMessage>
0556	<ResponseHeader>
0557	<ProtocolVersion>
0558	<ProtocolVersionMajor type="Integer" value="1"/>
0559	<ProtocolVersionMinor type="Integer" value="2"/>
0560	</ProtocolVersion>
0561	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0562	<BatchCount type="Integer" value="1"/>
0563	</ResponseHeader>
0564	<BatchItem>
0565	<Operation type="Enumeration" value="Destroy"/>
0566	<ResultStatus type="Enumeration" value="Success"/>
0567	<ResponsePayload>
0568	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0569	</ResponsePayload>
0570	</BatchItem>
0571	</ResponseMessage>
	# TIME 14
0572	<RequestMessage>
0573	<RequestHeader>
0574	<ProtocolVersion>
0575	<ProtocolVersionMajor type="Integer" value="1"/>
0576	<ProtocolVersionMinor type="Integer" value="2"/>
0577	</ProtocolVersion>
0578	<BatchCount type="Integer" value="1"/>
0579	</RequestHeader>
0580	<BatchItem>
0581	<Operation type="Enumeration" value="Destroy"/>
0582	<RequestPayload>
0583	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_5"/>
0584	</RequestPayload>
0585	</BatchItem>
0586	</RequestMessage>
0587	<ResponseMessage>
0588	<ResponseHeader>
0589	<ProtocolVersion>
0590	<ProtocolVersionMajor type="Integer" value="1"/>
0591	<ProtocolVersionMinor type="Integer" value="2"/>
0592	</ProtocolVersion>
0593	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0594	<BatchCount type="Integer" value="1"/>

0595	</ResponseHeader>
0596	<BatchItem>
0597	<Operation type="Enumeration" value="Destroy"/>
0598	<ResultStatus type="Enumeration" value="Success"/>
0599	<ResponsePayload>
0600	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_5"/>
0601	</ResponsePayload>
0602	</BatchItem>
0603	</ResponseMessage>

1224

1225 2.3.48 TC-SJ-3-12 - Join Split Keys

1226 Register split keys and join in various combinations.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SplitKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="x-ID"/>
0016	<AttributeValue type="TextString" value="TC-SJ-3-12-
	split1"/>
0017	</Attribute>
0018	</TemplateAttribute>
0019	<SplitKey>
0020	<SplitKeyParts type="Integer" value="4"/>
0021	<KeyPartIdentifier type="Integer" value="1"/>
0022	<SplitKeyThreshold type="Integer" value="2"/>
0023	<SplitKeyMethod type="Enumeration"
0024	value="PolynomialSharingGF2_8"/>
0025	<KeyBlock>
0026	<KeyFormatType type="Enumeration" value="Raw"/>
0027	<KeyValue>
	<KeyMaterial type="ByteString"
0028	value="66C46A7754F94DE420C7B1A7FFF5EC56"/>
0029	</KeyValue>
0030	</KeyBlock>
0031	</SplitKey>
0032	</RequestPayload>
0033	</BatchItem>
	</RequestMessage>
0034	<ResponseMessage>
0035	<ResponseHeader>
0036	<ProtocolVersion>

0037	<ProtocolVersionMajor type="Integer" value="1"/>
0038	<ProtocolVersionMinor type="Integer" value="2"/>
0039	</ProtocolVersion>
0040	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0041	<BatchCount type="Integer" value="1"/>
0042	</ResponseHeader>
0043	<BatchItem>
0044	<Operation type="Enumeration" value="Register"/>
0045	<ResultStatus type="Enumeration" value="Success"/>
0046	<ResponsePayload>
0047	<UniqueIdentifier type="TextString"
0048	value="\$UNIQUE_IDENTIFIER_0"/>
0049	</ResponsePayload>
0050	</BatchItem>
0051	</ResponseMessage>
# TIME 1	
0051	<RequestMessage>
0052	<RequestHeader>
0053	<ProtocolVersion>
0054	<ProtocolVersionMajor type="Integer" value="1"/>
0055	<ProtocolVersionMinor type="Integer" value="2"/>
0056	</ProtocolVersion>
0057	<BatchCount type="Integer" value="1"/>
0058	</RequestHeader>
0059	<BatchItem>
0060	<Operation type="Enumeration" value="Register"/>
0061	<RequestPayload>
0062	<ObjectType type="Enumeration" value="SplitKey"/>
0063	<TemplateAttribute>
0064	<Attribute>
0065	<AttributeName type="TextString" value="x-ID"/>
0066	<AttributeValue type="TextString" value="TC-SJ-3-12-
0067	split2"/>
0068	</Attribute>
0069	</TemplateAttribute>
0070	<SplitKey>
0071	<SplitKeyParts type="Integer" value="4"/>
0072	<KeyPartIdentifier type="Integer" value="2"/>
0073	<SplitKeyThreshold type="Integer" value="2"/>
0074	<SplitKeyMethod type="Enumeration"
0075	value="PolynomialSharingGF2_8"/>
0076	<KeyBlock>
0077	<KeyFormatType type="Enumeration" value="Raw"/>
0078	<KeyValue>
0079	<KeyMaterial type="ByteString"
0080	value="CF93D1E2A7E593CD5B8D6247F4E5D49C"/>
0081	</KeyValue>
0082	</KeyBlock>
0083	</SplitKey>
0084	</RequestPayload>
0085	</BatchItem>
0086	</RequestMessage>
0087	<ResponseMessage>
0088	<ResponseHeader>
0089	<ProtocolVersion>
0090	<ProtocolVersionMajor type="Integer" value="1"/>
0091	<ProtocolVersionMinor type="Integer" value="2"/>

0089	</ProtocolVersion>
0090	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0091	<BatchCount type="Integer" value="1"/>
0092	</ResponseHeader>
0093	<BatchItem>
0094	<Operation type="Enumeration" value="Register"/>
0095	<ResultStatus type="Enumeration" value="Success"/>
0096	<ResponsePayload>
0097	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0098	</ResponsePayload>
0099	</BatchItem>
0100	</ResponseMessage>
# TIME 2	
0101	<RequestMessage>
0102	<RequestHeader>
0103	<ProtocolVersion>
0104	<ProtocolVersionMajor type="Integer" value="1"/>
0105	<ProtocolVersionMinor type="Integer" value="2"/>
0106	</ProtocolVersion>
0107	<BatchCount type="Integer" value="1"/>
0108	</RequestHeader>
0109	<BatchItem>
0110	<Operation type="Enumeration" value="Register"/>
0111	<RequestPayload>
0112	<ObjectType type="Enumeration" value="SplitKey"/>
0113	<TemplateAttribute>
0114	<Attribute>
0115	<AttributeName type="TextString" value="x-ID"/>
0116	<AttributeValue type="TextString" value="TC-SJ-3-12-
	split3"/>
0117	</Attribute>
0118	</TemplateAttribute>
0119	<SplitKey>
0120	<SplitKeyParts type="Integer" value="4"/>
0121	<KeyPartIdentifier type="Integer" value="3"/>
0122	<SplitKeyThreshold type="Integer" value="2"/>
0123	<SplitKeyMethod type="Enumeration"
0124	value="PolynomialSharingGF2_8"/>
0125	<KeyBlock>
0126	<KeyFormatType type="Enumeration" value="Raw"/>
0127	<KeyValue>
	<KeyMaterial type="ByteString"
0128	value="A855B891F61AD9217240D8EC061E37DA"/>
0129	</KeyValue>
0130	</KeyBlock>
0131	</SplitKey>
0132	</RequestPayload>
0133	</BatchItem>
	</RequestMessage>
0134	<ResponseMessage>
0135	<ResponseHeader>
0136	<ProtocolVersion>
0137	<ProtocolVersionMajor type="Integer" value="1"/>
0138	<ProtocolVersionMinor type="Integer" value="2"/>
0139	</ProtocolVersion>
0140	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>

0141	<BatchCount type="Integer" value="1"/>
0142	</ResponseHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="Register"/>
0145	<ResultStatus type="Enumeration" value="Success"/>
0146	<ResponsePayload>
0147	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0148	</ResponsePayload>
0149	</BatchItem>
0150	</ResponseMessage>
0151	# TIME 3
0152	<RequestMessage>
0153	<RequestHeader>
0154	<ProtocolVersion>
0155	<ProtocolVersionMajor type="Integer" value="1"/>
0156	<ProtocolVersionMinor type="Integer" value="2"/>
0157	</ProtocolVersion>
0158	<BatchCount type="Integer" value="1"/>
0159	</RequestHeader>
0160	<BatchItem>
0161	<Operation type="Enumeration" value="Register"/>
0162	<RequestPayload>
0163	<ObjectType type="Enumeration" value="SplitKey"/>
0164	<TemplateAttribute>
0165	<Attribute>
0166	<AttributeName type="TextString" value="x-ID"/>
	<AttributeValue type="TextString" value="TC-SJ-3-12-
0167	split4"/>
0168	</Attribute>
0169	</TemplateAttribute>
0170	<SplitKey>
0171	<SplitKeyParts type="Integer" value="4"/>
0172	<KeyPartIdentifier type="Integer" value="4"/>
0173	<SplitKeyThreshold type="Integer" value="2"/>
0174	<SplitKeyMethod type="Enumeration"
0175	value="PolynomialSharingGF2_8"/>
0176	<KeyBlock>
0177	<KeyFormatType type="Enumeration" value="Raw"/>
0178	<KeyValue>
0179	<KeyMaterial type="ByteString"
0180	value="803DBAD55CDD329FAD19D99AE2C5A415"/>
0181	</KeyValue>
0182	</KeyBlock>
0183	</SplitKey>
	</RequestPayload>
	</BatchItem>
	</RequestMessage>
0184	<ResponseMessage>
0185	<ResponseHeader>
0186	<ProtocolVersion>
0187	<ProtocolVersionMajor type="Integer" value="1"/>
0188	<ProtocolVersionMinor type="Integer" value="2"/>
0189	</ProtocolVersion>
0190	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0191	<BatchCount type="Integer" value="1"/>
0192	</ResponseHeader>

0193	<BatchItem>
0194	<Operation type="Enumeration" value="Register"/>
0195	<ResultStatus type="Enumeration" value="Success"/>
0196	<ResponsePayload>
0197	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0198	</ResponsePayload>
0199	</BatchItem>
0200	</ResponseMessage>
	<i># TIME 4</i>
	<i># Successful Join with 2 of the required 2-of-4 keys</i>
0201	<RequestMessage>
0202	<RequestHeader>
0203	<ProtocolVersion>
0204	<ProtocolVersionMajor type="Integer" value="1"/>
0205	<ProtocolVersionMinor type="Integer" value="2"/>
0206	</ProtocolVersion>
0207	<BatchCount type="Integer" value="1"/>
0208	</RequestHeader>
0209	<BatchItem>
0210	<Operation type="Enumeration" value="JoinSplitKey"/>
0211	<RequestPayload>
0212	<ObjectType type="Enumeration" value="SymmetricKey"/>
0213	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0214	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0215	<TemplateAttribute>
0216	<Attribute>
0217	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0218	<AttributeValue type="Enumeration" value="AES"/>
0219	</Attribute>
0220	<Attribute>
0221	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0222	<AttributeValue type="Integer" value="128"/>
0223	</Attribute>
0224	<Attribute>
0225	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>
0226	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0227	</Attribute>
0228	<Attribute>
0229	<AttributeName type="TextString" value="Name"/>
0230	<AttributeValue>
0231	<NameValue type="TextString" value="TC-SJ-3-12-join1"/>
0232	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0233	</AttributeValue>
0234	</Attribute>
0235	</TemplateAttribute>
0236	</RequestPayload>
0237	</BatchItem>
0238	</RequestMessage>
0239	<ResponseMessage>
0240	<ResponseHeader>

0241	<ProtocolVersion>
0242	<ProtocolVersionMajor type="Integer" value="1"/>
0243	<ProtocolVersionMinor type="Integer" value="2"/>
0244	</ProtocolVersion>
0245	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0246	<BatchCount type="Integer" value="1"/>
0247	</ResponseHeader>
0248	<BatchItem>
0249	<Operation type="Enumeration" value="JoinSplitKey"/>
0250	<ResultStatus type="Enumeration" value="Success"/>
0251	<ResponsePayload>
0252	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0253	</ResponsePayload>
0254	</BatchItem>
0255	</ResponseMessage>
# TIME 5	
0256	<RequestMessage>
0257	<RequestHeader>
0258	<ProtocolVersion>
0259	<ProtocolVersionMajor type="Integer" value="1"/>
0260	<ProtocolVersionMinor type="Integer" value="2"/>
0261	</ProtocolVersion>
0262	<BatchCount type="Integer" value="1"/>
0263	</RequestHeader>
0264	<BatchItem>
0265	<Operation type="Enumeration" value="Get"/>
0266	<RequestPayload>
0267	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0268	</RequestPayload>
0269	</BatchItem>
0270	</RequestMessage>
0271	<ResponseMessage>
0272	<ResponseHeader>
0273	<ProtocolVersion>
0274	<ProtocolVersionMajor type="Integer" value="1"/>
0275	<ProtocolVersionMinor type="Integer" value="2"/>
0276	</ProtocolVersion>
0277	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0278	<BatchCount type="Integer" value="1"/>
0279	</ResponseHeader>
0280	<BatchItem>
0281	<Operation type="Enumeration" value="Get"/>
0282	<ResultStatus type="Enumeration" value="Success"/>
0283	<ResponsePayload>
0284	<ObjectType type="Enumeration" value="SymmetricKey"/>
0285	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0286	<SymmetricKey>
0287	<KeyBlock>
0288	<KeyFormatType type="Enumeration" value="Raw"/>
0289	<KeyValue>
0290	<KeyMaterial type="ByteString"
	value="0102030405060708090a0b0c0d0e0f10"/>
0291	</KeyValue>
0292	<CryptographicAlgorithm type="Enumeration" value="AES"/>

0293	<CryptographicLength type="Integer" value="128"/>
0294	</KeyBlock>
0295	</SymmetricKey>
0296	</ResponsePayload>
0297	</BatchItem>
0298	</ResponseMessage>
# TIME 6 # Non-successful Join with only 1 of the required 2-of-4 keys	
0299	<RequestMessage>
0300	<RequestHeader>
0301	<ProtocolVersion>
0302	<ProtocolVersionMajor type="Integer" value="1"/>
0303	<ProtocolVersionMinor type="Integer" value="2"/>
0304	</ProtocolVersion>
0305	<BatchCount type="Integer" value="1"/>
0306	</RequestHeader>
0307	<BatchItem>
0308	<Operation type="Enumeration" value="JoinSplitKey"/>
0309	<RequestPayload>
0310	<ObjectType type="Enumeration" value="SymmetricKey"/>
0311	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0312	</RequestPayload>
0313	</BatchItem>
0314	</RequestMessage>
0315	<ResponseMessage>
0316	<ResponseHeader>
0317	<ProtocolVersion>
0318	<ProtocolVersionMajor type="Integer" value="1"/>
0319	<ProtocolVersionMinor type="Integer" value="2"/>
0320	</ProtocolVersion>
0321	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0322	<BatchCount type="Integer" value="1"/>
0323	</ResponseHeader>
0324	<BatchItem>
0325	<Operation type="Enumeration" value="JoinSplitKey"/>
0326	<ResultStatus type="Enumeration" value="OperationFailed"/>
0327	<ResultReason type="Enumeration" value="CryptographicFailure"/>
0328	<ResultMessage type="TextString" value="FAILURE"/>
0329	</BatchItem>
0330	</ResponseMessage>
# TIME 7	
0331	<RequestMessage>
0332	<RequestHeader>
0333	<ProtocolVersion>
0334	<ProtocolVersionMajor type="Integer" value="1"/>
0335	<ProtocolVersionMinor type="Integer" value="2"/>
0336	</ProtocolVersion>
0337	<BatchCount type="Integer" value="1"/>
0338	</RequestHeader>
0339	<BatchItem>
0340	<Operation type="Enumeration" value="Destroy"/>
0341	<RequestPayload>
0342	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0343	</RequestPayload>

0344	</BatchItem>
0345	</RequestMessage>
0346	<ResponseMessage>
0347	<ResponseHeader>
0348	<ProtocolVersion>
0349	<ProtocolVersionMajor type="Integer" value="1"/>
0350	<ProtocolVersionMinor type="Integer" value="2"/>
0351	</ProtocolVersion>
0352	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0353	<BatchCount type="Integer" value="1"/>
0354	</ResponseHeader>
0355	<BatchItem>
0356	<Operation type="Enumeration" value="Destroy"/>
0357	<ResultStatus type="Enumeration" value="Success"/>
0358	<ResponsePayload>
0359	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0360	</ResponsePayload>
0361	</BatchItem>
0362	</ResponseMessage>
	# TIME 8
0363	<RequestMessage>
0364	<RequestHeader>
0365	<ProtocolVersion>
0366	<ProtocolVersionMajor type="Integer" value="1"/>
0367	<ProtocolVersionMinor type="Integer" value="2"/>
0368	</ProtocolVersion>
0369	<BatchCount type="Integer" value="1"/>
0370	</RequestHeader>
0371	<BatchItem>
0372	<Operation type="Enumeration" value="Destroy"/>
0373	<RequestPayload>
0374	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0375	</RequestPayload>
0376	</BatchItem>
0377	</RequestMessage>
0378	<ResponseMessage>
0379	<ResponseHeader>
0380	<ProtocolVersion>
0381	<ProtocolVersionMajor type="Integer" value="1"/>
0382	<ProtocolVersionMinor type="Integer" value="2"/>
0383	</ProtocolVersion>
0384	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0385	<BatchCount type="Integer" value="1"/>
0386	</ResponseHeader>
0387	<BatchItem>
0388	<Operation type="Enumeration" value="Destroy"/>
0389	<ResultStatus type="Enumeration" value="Success"/>
0390	<ResponsePayload>
0391	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0392	</ResponsePayload>
0393	</BatchItem>
0394	</ResponseMessage>
	# TIME 9

0395	<RequestMessage>
0396	<RequestHeader>
0397	<ProtocolVersion>
0398	<ProtocolVersionMajor type="Integer" value="1"/>
0399	<ProtocolVersionMinor type="Integer" value="2"/>
0400	</ProtocolVersion>
0401	<BatchCount type="Integer" value="1"/>
0402	</RequestHeader>
0403	<BatchItem>
0404	<Operation type="Enumeration" value="Destroy"/>
0405	<RequestPayload>
0406	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0407	</RequestPayload>
0408	</BatchItem>
0409	</RequestMessage>
0410	<ResponseMessage>
0411	<ResponseHeader>
0412	<ProtocolVersion>
0413	<ProtocolVersionMajor type="Integer" value="1"/>
0414	<ProtocolVersionMinor type="Integer" value="2"/>
0415	</ProtocolVersion>
0416	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0417	<BatchCount type="Integer" value="1"/>
0418	</ResponseHeader>
0419	<BatchItem>
0420	<Operation type="Enumeration" value="Destroy"/>
0421	<ResultStatus type="Enumeration" value="Success"/>
0422	<ResponsePayload>
0423	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0424	</ResponsePayload>
0425	</BatchItem>
0426	</ResponseMessage>
	# TIME 10
0427	<RequestMessage>
0428	<RequestHeader>
0429	<ProtocolVersion>
0430	<ProtocolVersionMajor type="Integer" value="1"/>
0431	<ProtocolVersionMinor type="Integer" value="2"/>
0432	</ProtocolVersion>
0433	<BatchCount type="Integer" value="1"/>
0434	</RequestHeader>
0435	<BatchItem>
0436	<Operation type="Enumeration" value="Destroy"/>
0437	<RequestPayload>
0438	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0439	</RequestPayload>
0440	</BatchItem>
0441	</RequestMessage>
0442	<ResponseMessage>
0443	<ResponseHeader>
0444	<ProtocolVersion>
0445	<ProtocolVersionMajor type="Integer" value="1"/>
0446	<ProtocolVersionMinor type="Integer" value="2"/>

0447	</ProtocolVersion>
0448	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0449	<BatchCount type="Integer" value="1"/>
0450	</ResponseHeader>
0451	<BatchItem>
0452	<Operation type="Enumeration" value="Destroy"/>
0453	<ResultStatus type="Enumeration" value="Success"/>
0454	<ResponsePayload>
0455	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0456	</ResponsePayload>
0457	</BatchItem>
0458	</ResponseMessage>
# TIME 11	
0459	<RequestMessage>
0460	<RequestHeader>
0461	<ProtocolVersion>
0462	<ProtocolVersionMajor type="Integer" value="1"/>
0463	<ProtocolVersionMinor type="Integer" value="2"/>
0464	</ProtocolVersion>
0465	<BatchCount type="Integer" value="1"/>
0466	</RequestHeader>
0467	<BatchItem>
0468	<Operation type="Enumeration" value="Destroy"/>
0469	<RequestPayload>
0470	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0471	</RequestPayload>
0472	</BatchItem>
0473	</RequestMessage>
0474	<ResponseMessage>
0475	<ResponseHeader>
0476	<ProtocolVersion>
0477	<ProtocolVersionMajor type="Integer" value="1"/>
0478	<ProtocolVersionMinor type="Integer" value="2"/>
0479	</ProtocolVersion>
0480	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0481	<BatchCount type="Integer" value="1"/>
0482	</ResponseHeader>
0483	<BatchItem>
0484	<Operation type="Enumeration" value="Destroy"/>
0485	<ResultStatus type="Enumeration" value="Success"/>
0486	<ResponsePayload>
0487	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0488	</ResponsePayload>
0489	</BatchItem>
0490	</ResponseMessage>

1227

1228 2.3.49 TC-SJ-4-12 - Register and Split / Join with XOR

1229 Register a symmetric key and perform split and join in various combinations.

# TIME 0	
0001	<RequestMessage>

0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Register"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0016	<AttributeValue type="Integer" value="Encrypt Decrypt"/>
0017	</Attribute>
0018	<Attribute>
0019	<AttributeName type="TextString" value="x-ID"/>
0020	<AttributeValue type="TextString" value="TC-SJ-4-12"/>
0021	</Attribute>
0022	</TemplateAttribute>
0023	<SymmetricKey>
0024	<KeyBlock>
0025	<KeyFormatType type="Enumeration" value="Raw"/>
0026	<KeyValue>
0027	<KeyMaterial type="ByteString" value="0102030405060708090a0b0c0d0e0f10"/>
0028	</KeyValue>
0029	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0030	<CryptographicLength type="Integer" value="128"/>
0031	</KeyBlock>
0032	</SymmetricKey>
0033	</RequestPayload>
0034	</BatchItem>
0035	</RequestMessage>
0036	<ResponseMessage>
0037	<ResponseHeader>
0038	<ProtocolVersion>
0039	<ProtocolVersionMajor type="Integer" value="1"/>
0040	<ProtocolVersionMinor type="Integer" value="2"/>
0041	</ProtocolVersion>
0042	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0043	<BatchCount type="Integer" value="1"/>
0044	</ResponseHeader>
0045	<BatchItem>
0046	<Operation type="Enumeration" value="Register"/>
0047	<ResultStatus type="Enumeration" value="Success"/>
0048	<ResponsePayload>
0049	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0050	</ResponsePayload>
0051	</BatchItem>
0052	</ResponseMessage>
	# TIME 1
0053	<RequestMessage>
0054	<RequestHeader>

0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="2"/>
0058	</ProtocolVersion>
0059	<BatchCount type="Integer" value="1"/>
0060	</RequestHeader>
0061	<BatchItem>
0062	<Operation type="Enumeration" value="CreateSplitKey"/>
0063	<RequestPayload>
0064	<ObjectType type="Enumeration" value="SplitKey"/>
0065	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0066	<SplitKeyParts type="Integer" value="4"/>
0067	<SplitKeyThreshold type="Integer" value="4"/>
0068	<SplitKeyMethod type="Enumeration" value="XOR"/>
0069	<TemplateAttribute>
0070	</TemplateAttribute>
0071	</RequestPayload>
0072	</BatchItem>
0073	</RequestMessage>
0074	<ResponseMessage>
0075	<ResponseHeader>
0076	<ProtocolVersion>
0077	<ProtocolVersionMajor type="Integer" value="1"/>
0078	<ProtocolVersionMinor type="Integer" value="2"/>
0079	</ProtocolVersion>
0080	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0081	<BatchCount type="Integer" value="1"/>
0082	</ResponseHeader>
0083	<BatchItem>
0084	<Operation type="Enumeration" value="CreateSplitKey"/>
0085	<ResultStatus type="Enumeration" value="Success"/>
0086	<ResponsePayload>
0087	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0088	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0089	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0090	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0091	</ResponsePayload>
0092	</BatchItem>
0093	</ResponseMessage>
	# TIME 2
0094	<RequestMessage>
0095	<RequestHeader>
0096	<ProtocolVersion>
0097	<ProtocolVersionMajor type="Integer" value="1"/>
0098	<ProtocolVersionMinor type="Integer" value="2"/>
0099	</ProtocolVersion>
0100	<BatchCount type="Integer" value="1"/>
0101	</RequestHeader>
0102	<BatchItem>
0103	<Operation type="Enumeration" value="Get"/>
0104	<RequestPayload>
0105	<UniqueIdentifier type="TextString"

0106	value="\$UNIQUE_IDENTIFIER_1"/>
0107	</RequestPayload>
0108	</BatchItem>
0109	</RequestMessage>
0109	<ResponseMessage>
0110	<ResponseHeader>
0111	<ProtocolVersion>
0112	<ProtocolVersionMajor type="Integer" value="1"/>
0113	<ProtocolVersionMinor type="Integer" value="2"/>
0114	</ProtocolVersion>
0115	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0116	<BatchCount type="Integer" value="1"/>
0117	</ResponseHeader>
0118	<BatchItem>
0119	<Operation type="Enumeration" value="Get"/>
0120	<ResultStatus type="Enumeration" value="Success"/>
0121	<ResponsePayload>
0122	<ObjectType type="Enumeration" value="SplitKey"/>
0123	<UniqueIdentifier type="TextString"
0124	value="\$UNIQUE_IDENTIFIER_1"/>
0125	<SplitKey>
0126	<SplitKeyParts type="Integer" value="4"/>
0127	<KeyPartIdentifier type="Integer" value="1"/>
0128	<SplitKeyThreshold type="Integer" value="4"/>
0129	<SplitKeyMethod type="Enumeration" value="XOR"/>
0130	<KeyBlock>
0131	<KeyFormatType type="Enumeration" value="Raw"/>
0132	<KeyValue>
0133	<KeyMaterial type="ByteString"
0134	value="d4b92c299199298e30dee13b967e6dda"/>
0135	</KeyValue>
0136	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0137	<CryptographicLength type="Integer" value="128"/>
0138	</KeyBlock>
0139	</SplitKey>
0140	</ResponsePayload>
0141	</BatchItem>
0142	</ResponseMessage>
0141	# TIME 3
0141	<RequestMessage>
0142	<RequestHeader>
0143	<ProtocolVersion>
0144	<ProtocolVersionMajor type="Integer" value="1"/>
0145	<ProtocolVersionMinor type="Integer" value="2"/>
0146	</ProtocolVersion>
0147	<BatchCount type="Integer" value="1"/>
0148	</RequestHeader>
0149	<BatchItem>
0150	<Operation type="Enumeration" value="Get"/>
0151	<RequestPayload>
0152	<UniqueIdentifier type="TextString"
0153	value="\$UNIQUE_IDENTIFIER_2"/>
0154	</RequestPayload>
0155	</BatchItem>
0156	</RequestMessage>
0156	<ResponseMessage>

0157	<ResponseHeader>
0158	<ProtocolVersion>
0159	<ProtocolVersionMajor type="Integer" value="1"/>
0160	<ProtocolVersionMinor type="Integer" value="2"/>
0161	</ProtocolVersion>
0162	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0163	<BatchCount type="Integer" value="1"/>
0164	</ResponseHeader>
0165	<BatchItem>
0166	<Operation type="Enumeration" value="Get"/>
0167	<ResultStatus type="Enumeration" value="Success"/>
0168	<ResponsePayload>
0169	<ObjectType type="Enumeration" value="SplitKey"/>
0170	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0171	<SplitKey>
0172	<SplitKeyParts type="Integer" value="4"/>
0173	<KeyPartIdentifier type="Integer" value="2"/>
0174	<SplitKeyThreshold type="Integer" value="4"/>
0175	<SplitKeyMethod type="Enumeration" value="XOR"/>
0176	<KeyBlock>
0177	<KeyFormatType type="Enumeration" value="Raw"/>
0178	<KeyValue>
0179	<KeyMaterial type="ByteString"
	value="35ea4f615686230c7b11538693674e89"/>
0180	</KeyValue>
0181	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0182	<CryptographicLength type="Integer" value="128"/>
0183	</KeyBlock>
0184	</SplitKey>
0185	</ResponsePayload>
0186	</BatchItem>
0187	</ResponseMessage>
	# TIME 4
0188	<RequestMessage>
0189	<RequestHeader>
0190	<ProtocolVersion>
0191	<ProtocolVersionMajor type="Integer" value="1"/>
0192	<ProtocolVersionMinor type="Integer" value="2"/>
0193	</ProtocolVersion>
0194	<BatchCount type="Integer" value="1"/>
0195	</RequestHeader>
0196	<BatchItem>
0197	<Operation type="Enumeration" value="Get"/>
0198	<RequestPayload>
0199	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0200	</RequestPayload>
0201	</BatchItem>
0202	</RequestMessage>
0203	<ResponseMessage>
0204	<ResponseHeader>
0205	<ProtocolVersion>
0206	<ProtocolVersionMajor type="Integer" value="1"/>
0207	<ProtocolVersionMinor type="Integer" value="2"/>
0208	</ProtocolVersion>
0209	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>

0210	<BatchCount type="Integer" value="1"/>
0211	</ResponseHeader>
0212	<BatchItem>
0213	<Operation type="Enumeration" value="Get"/>
0214	<ResultStatus type="Enumeration" value="Success"/>
0215	<ResponsePayload>
0216	<ObjectType type="Enumeration" value="SplitKey"/>
0217	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0218	<SplitKey>
0219	<SplitKeyParts type="Integer" value="4"/>
0220	<KeyPartIdentifier type="Integer" value="3"/>
0221	<SplitKeyThreshold type="Integer" value="4"/>
0222	<SplitKeyMethod type="Enumeration" value="XOR"/>
0223	<KeyBlock>
0224	<KeyFormatType type="Enumeration" value="Raw"/>
0225	<KeyValue>
0226	<KeyMaterial type="ByteString"
	value="3478ddd2e1f89f2005011d26d9fff37c"/>
0227	</KeyValue>
0228	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0229	<CryptographicLength type="Integer" value="128"/>
0230	</KeyBlock>
0231	</SplitKey>
0232	</ResponsePayload>
0233	</BatchItem>
0234	</ResponseMessage>
	# TIME 5
0235	<RequestMessage>
0236	<RequestHeader>
0237	<ProtocolVersion>
0238	<ProtocolVersionMajor type="Integer" value="1"/>
0239	<ProtocolVersionMinor type="Integer" value="2"/>
0240	</ProtocolVersion>
0241	<BatchCount type="Integer" value="1"/>
0242	</RequestHeader>
0243	<BatchItem>
0244	<Operation type="Enumeration" value="Get"/>
0245	<RequestPayload>
0246	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0247	</RequestPayload>
0248	</BatchItem>
0249	</RequestMessage>
0250	<ResponseMessage>
0251	<ResponseHeader>
0252	<ProtocolVersion>
0253	<ProtocolVersionMajor type="Integer" value="1"/>
0254	<ProtocolVersionMinor type="Integer" value="2"/>
0255	</ProtocolVersion>
0256	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0257	<BatchCount type="Integer" value="1"/>
0258	</ResponseHeader>
0259	<BatchItem>
0260	<Operation type="Enumeration" value="Get"/>
0261	<ResultStatus type="Enumeration" value="Success"/>
0262	<ResponsePayload>

0263	<ObjectType type="Enumeration" value="SplitKey"/>
0264	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0265	<SplitKey>
0266	<SplitKeyParts type="Integer" value="4"/>
0267	<KeyPartIdentifier type="Integer" value="4"/>
0268	<SplitKeyThreshold type="Integer" value="4"/>
0269	<SplitKeyMethod type="Enumeration" value="XOR"/>
0270	<KeyBlock>
0271	<KeyFormatType type="Enumeration" value="Raw"/>
0272	<KeyValue>
0273	<KeyMaterial type="ByteString"
	value="d429bd9e23e192aa47c4a497d1e8df3f"/>
0274	</KeyValue>
0275	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0276	<CryptographicLength type="Integer" value="128"/>
0277	</KeyBlock>
0278	</SplitKey>
0279	</ResponsePayload>
0280	</BatchItem>
0281	</ResponseMessage>
	<i># TIME 6</i>
	<i># Successful Join with 4 of the required 4-of-4 keys</i>
0282	<RequestMessage>
0283	<RequestHeader>
0284	<ProtocolVersion>
0285	<ProtocolVersionMajor type="Integer" value="1"/>
0286	<ProtocolVersionMinor type="Integer" value="2"/>
0287	</ProtocolVersion>
0288	<BatchCount type="Integer" value="1"/>
0289	</RequestHeader>
0290	<BatchItem>
0291	<Operation type="Enumeration" value="JoinSplitKey"/>
0292	<RequestPayload>
0293	<ObjectType type="Enumeration" value="SymmetricKey"/>
0294	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0295	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0296	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0297	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0298	<TemplateAttribute>
0299	<Attribute>
0300	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0301	<AttributeValue type="Enumeration" value="AES"/>
0302	</Attribute>
0303	<Attribute>
0304	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0305	<AttributeValue type="Integer" value="128"/>
0306	</Attribute>
0307	<Attribute>
0308	<AttributeName type="TextString" value="Cryptographic
	Usage Mask"/>

0309	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0310	</Attribute>
0311	<Attribute>
0312	<AttributeName type="TextString" value="Name"/>
0313	<AttributeValue>
0314	<NameValue type="TextString" value="TC-SJ-4-12-join1"/>
0315	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0316	</AttributeValue>
0317	</Attribute>
0318	</TemplateAttribute>
0319	</RequestPayload>
0320	</BatchItem>
0321	</RequestMessage>
0322	<ResponseMessage>
0323	<ResponseHeader>
0324	<ProtocolVersion>
0325	<ProtocolVersionMajor type="Integer" value="1"/>
0326	<ProtocolVersionMinor type="Integer" value="2"/>
0327	</ProtocolVersion>
0328	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0329	<BatchCount type="Integer" value="1"/>
0330	</ResponseHeader>
0331	<BatchItem>
0332	<Operation type="Enumeration" value="JoinSplitKey"/>
0333	<ResultStatus type="Enumeration" value="Success"/>
0334	<ResponsePayload>
0335	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_5"/>
0336	</ResponsePayload>
0337	</BatchItem>
0338	</ResponseMessage>
	# TIME 7
0339	<RequestMessage>
0340	<RequestHeader>
0341	<ProtocolVersion>
0342	<ProtocolVersionMajor type="Integer" value="1"/>
0343	<ProtocolVersionMinor type="Integer" value="2"/>
0344	</ProtocolVersion>
0345	<BatchCount type="Integer" value="1"/>
0346	</RequestHeader>
0347	<BatchItem>
0348	<Operation type="Enumeration" value="Get"/>
0349	<RequestPayload>
0350	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_5"/>
0351	</RequestPayload>
0352	</BatchItem>
0353	</RequestMessage>
0354	<ResponseMessage>
0355	<ResponseHeader>
0356	<ProtocolVersion>
0357	<ProtocolVersionMajor type="Integer" value="1"/>
0358	<ProtocolVersionMinor type="Integer" value="2"/>
0359	</ProtocolVersion>
0360	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>

0361	<BatchCount type="Integer" value="1"/>
0362	</ResponseHeader>
0363	<BatchItem>
0364	<Operation type="Enumeration" value="Get"/>
0365	<ResultStatus type="Enumeration" value="Success"/>
0366	<ResponsePayload>
0367	<ObjectType type="Enumeration" value="SymmetricKey"/>
0368	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_5"/>
0369	<SymmetricKey>
0370	<KeyBlock>
0371	<KeyFormatType type="Enumeration" value="Raw"/>
0372	<KeyValue>
0373	<KeyMaterial type="ByteString"
	value="0102030405060708090a0b0c0d0e0f10"/>
0374	</KeyValue>
0375	<CryptographicAlgorithm type="Enumeration" value="AES"/>
0376	<CryptographicLength type="Integer" value="128"/>
0377	</KeyBlock>
0378	</SymmetricKey>
0379	</ResponsePayload>
0380	</BatchItem>
0381	</ResponseMessage>
	<i># TIME 8</i>
	<i># Non-successful Join with only 1 of the required 4-of-4 keys</i>
0382	<RequestMessage>
0383	<RequestHeader>
0384	<ProtocolVersion>
0385	<ProtocolVersionMajor type="Integer" value="1"/>
0386	<ProtocolVersionMinor type="Integer" value="2"/>
0387	</ProtocolVersion>
0388	<BatchCount type="Integer" value="1"/>
0389	</RequestHeader>
0390	<BatchItem>
0391	<Operation type="Enumeration" value="JoinSplitKey"/>
0392	<RequestPayload>
0393	<ObjectType type="Enumeration" value="SymmetricKey"/>
0394	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0395	</RequestPayload>
0396	</BatchItem>
0397	</RequestMessage>
0398	<ResponseMessage>
0399	<ResponseHeader>
0400	<ProtocolVersion>
0401	<ProtocolVersionMajor type="Integer" value="1"/>
0402	<ProtocolVersionMinor type="Integer" value="2"/>
0403	</ProtocolVersion>
0404	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0405	<BatchCount type="Integer" value="1"/>
0406	</ResponseHeader>
0407	<BatchItem>
0408	<Operation type="Enumeration" value="JoinSplitKey"/>
0409	<ResultStatus type="Enumeration" value="OperationFailed"/>
0410	<ResultReason type="Enumeration" value="CryptographicFailure"/>
0411	<ResultMessage type="TextString" value="FAILURE"/>
0412	</BatchItem>

0413	</ResponseMessage>
	# TIME 9
0414	<RequestMessage>
0415	<RequestHeader>
0416	<ProtocolVersion>
0417	<ProtocolVersionMajor type="Integer" value="1"/>
0418	<ProtocolVersionMinor type="Integer" value="2"/>
0419	</ProtocolVersion>
0420	<BatchCount type="Integer" value="1"/>
0421	</RequestHeader>
0422	<BatchItem>
0423	<Operation type="Enumeration" value="Destroy"/>
0424	<RequestPayload>
0425	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0426	</RequestPayload>
0427	</BatchItem>
0428	</RequestMessage>
0429	<ResponseMessage>
0430	<ResponseHeader>
0431	<ProtocolVersion>
0432	<ProtocolVersionMajor type="Integer" value="1"/>
0433	<ProtocolVersionMinor type="Integer" value="2"/>
0434	</ProtocolVersion>
0435	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0436	<BatchCount type="Integer" value="1"/>
0437	</ResponseHeader>
0438	<BatchItem>
0439	<Operation type="Enumeration" value="Destroy"/>
0440	<ResultStatus type="Enumeration" value="Success"/>
0441	<ResponsePayload>
0442	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0443	</ResponsePayload>
0444	</BatchItem>
0445	</ResponseMessage>
	# TIME 10
0446	<RequestMessage>
0447	<RequestHeader>
0448	<ProtocolVersion>
0449	<ProtocolVersionMajor type="Integer" value="1"/>
0450	<ProtocolVersionMinor type="Integer" value="2"/>
0451	</ProtocolVersion>
0452	<BatchCount type="Integer" value="1"/>
0453	</RequestHeader>
0454	<BatchItem>
0455	<Operation type="Enumeration" value="Destroy"/>
0456	<RequestPayload>
0457	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0458	</RequestPayload>
0459	</BatchItem>
0460	</RequestMessage>
0461	<ResponseMessage>
0462	<ResponseHeader>
0463	<ProtocolVersion>

0464	<ProtocolVersionMajor type="Integer" value="1"/>
0465	<ProtocolVersionMinor type="Integer" value="2"/>
0466	</ProtocolVersion>
0467	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0468	<BatchCount type="Integer" value="1"/>
0469	</ResponseHeader>
0470	<BatchItem>
0471	<Operation type="Enumeration" value="Destroy"/>
0472	<ResultStatus type="Enumeration" value="Success"/>
0473	<ResponsePayload>
0474	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0475	</ResponsePayload>
0476	</BatchItem>
0477	</ResponseMessage>
# TIME 11	
0478	<RequestMessage>
0479	<RequestHeader>
0480	<ProtocolVersion>
0481	<ProtocolVersionMajor type="Integer" value="1"/>
0482	<ProtocolVersionMinor type="Integer" value="2"/>
0483	</ProtocolVersion>
0484	<BatchCount type="Integer" value="1"/>
0485	</RequestHeader>
0486	<BatchItem>
0487	<Operation type="Enumeration" value="Destroy"/>
0488	<RequestPayload>
0489	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0490	</RequestPayload>
0491	</BatchItem>
0492	</RequestMessage>
0493	<ResponseMessage>
0494	<ResponseHeader>
0495	<ProtocolVersion>
0496	<ProtocolVersionMajor type="Integer" value="1"/>
0497	<ProtocolVersionMinor type="Integer" value="2"/>
0498	</ProtocolVersion>
0499	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0500	<BatchCount type="Integer" value="1"/>
0501	</ResponseHeader>
0502	<BatchItem>
0503	<Operation type="Enumeration" value="Destroy"/>
0504	<ResultStatus type="Enumeration" value="Success"/>
0505	<ResponsePayload>
0506	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_2"/>
0507	</ResponsePayload>
0508	</BatchItem>
0509	</ResponseMessage>
# TIME 12	
0510	<RequestMessage>
0511	<RequestHeader>
0512	<ProtocolVersion>
0513	<ProtocolVersionMajor type="Integer" value="1"/>
0514	<ProtocolVersionMinor type="Integer" value="2"/>

0515	</ProtocolVersion>
0516	<BatchCount type="Integer" value="1"/>
0517	</RequestHeader>
0518	<BatchItem>
0519	<Operation type="Enumeration" value="Destroy"/>
0520	<RequestPayload>
0521	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0522	</RequestPayload>
0523	</BatchItem>
0524	</RequestMessage>
0525	<ResponseMessage>
0526	<ResponseHeader>
0527	<ProtocolVersion>
0528	<ProtocolVersionMajor type="Integer" value="1"/>
0529	<ProtocolVersionMinor type="Integer" value="2"/>
0530	</ProtocolVersion>
0531	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0532	<BatchCount type="Integer" value="1"/>
0533	</ResponseHeader>
0534	<BatchItem>
0535	<Operation type="Enumeration" value="Destroy"/>
0536	<ResultStatus type="Enumeration" value="Success"/>
0537	<ResponsePayload>
0538	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_3"/>
0539	</ResponsePayload>
0540	</BatchItem>
0541	</ResponseMessage>
0542	# TIME 13
0543	<RequestMessage>
0544	<RequestHeader>
0545	<ProtocolVersion>
0546	<ProtocolVersionMajor type="Integer" value="1"/>
0547	<ProtocolVersionMinor type="Integer" value="2"/>
0548	</ProtocolVersion>
0549	<BatchCount type="Integer" value="1"/>
0550	</RequestHeader>
0551	<BatchItem>
0552	<Operation type="Enumeration" value="Destroy"/>
0553	<RequestPayload>
	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0554	</RequestPayload>
0555	</BatchItem>
0556	</RequestMessage>
0557	<ResponseMessage>
0558	<ResponseHeader>
0559	<ProtocolVersion>
0560	<ProtocolVersionMajor type="Integer" value="1"/>
0561	<ProtocolVersionMinor type="Integer" value="2"/>
0562	</ProtocolVersion>
0563	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0564	<BatchCount type="Integer" value="1"/>
0565	</ResponseHeader>
0566	<BatchItem>

0567	<Operation type="Enumeration" value="Destroy"/>
0568	<ResultStatus type="Enumeration" value="Success"/>
0569	<ResponsePayload>
0570	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_4"/>
0571	</ResponsePayload>
0572	</BatchItem>
0573	</ResponseMessage>
	# TIME 14
0574	<RequestMessage>
0575	<RequestHeader>
0576	<ProtocolVersion>
0577	<ProtocolVersionMajor type="Integer" value="1"/>
0578	<ProtocolVersionMinor type="Integer" value="2"/>
0579	</ProtocolVersion>
0580	<BatchCount type="Integer" value="1"/>
0581	</RequestHeader>
0582	<BatchItem>
0583	<Operation type="Enumeration" value="Destroy"/>
0584	<RequestPayload>
0585	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_5"/>
0586	</RequestPayload>
0587	</BatchItem>
0588	</RequestMessage>
0589	<ResponseMessage>
0590	<ResponseHeader>
0591	<ProtocolVersion>
0592	<ProtocolVersionMajor type="Integer" value="1"/>
0593	<ProtocolVersionMinor type="Integer" value="2"/>
0594	</ProtocolVersion>
0595	<TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0596	<BatchCount type="Integer" value="1"/>
0597	</ResponseHeader>
0598	<BatchItem>
0599	<Operation type="Enumeration" value="Destroy"/>
0600	<ResultStatus type="Enumeration" value="Success"/>
0601	<ResponsePayload>
0602	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_5"/>
0603	</ResponsePayload>
0604	</BatchItem>
0605	</ResponseMessage>

1230

1231 Appendix A. Acknowledgments

1232 The following individuals have participated in the creation of this specification and are gratefully
1233 acknowledged:

1234 Editors of the previous versions of this document:

1235 Mathias Björkqvist, IBM (v1.0 and v1.1)
1236 Tim Hudson, Cryptsoft (v1.1)
1237 René Pawlitzek, IBM (v1.0)
1238

1239 Technical Committee Participants:

1240 Hal Aldridge, Sypris Electronics
1241 Mike Allen, Symantec
1242 Gordon Arnold, IBM
1243 Todd Arnold, IBM
1244 Richard Austin, Hewlett-Packard
1245 Lars Bagnert, PrimeKey
1246 Elaine Barker, NIST
1247 Peter Bartok, Venafi, Inc.
1248 Tom Benjamin, IBM
1249 Anthony Berglas, Cryptsoft
1250 Mathias Björkqvist, IBM
1251 Kevin Bocket, Venafi
1252 Anne Bolgert, IBM
1253 Alan Brown, Thales e-Security
1254 Tim Bruce, CA Technologies
1255 Chris Burchett, Credant Technologies, Inc.
1256 Kelley Burgin, National Security Agency
1257 Robert Burns, Thales e-Security
1258 Chuck Castleton, Venafi
1259 Kenli Chong, QuintessenceLabs
1260 John Clark, Hewlett-Packard
1261 Tom Clifford, Symantec Corp.
1262 Doron Cohen, SafeNet, Inc
1263 Tony Cox, Cryptsoft
1264 Russell Dietz, SafeNet, Inc
1265 Graydon Dodson, Lexmark International Inc.
1266 Vinod Duggirala, EMC Corporation
1267 Chris Dunn, SafeNet, Inc.
1268 Michael Duren, Sypris Electronics
1269 James Dzierzanowski, American Express CCoE
1270 Faisal Faruqui, Thales e-Security
1271 Stan Feather, Hewlett-Packard
1272 David Finkelstein, Symantec Corp.
1273 James Fitzgerald, SafeNet, Inc.
1274 Indra Fitzgerald, Hewlett-Packard
1275 Judith Furlong, EMC Corporation
1276 Susan Gleeson, Oracle
1277 Robert Griffin, EMC Corporation
1278 Paul Grojean, Individual
1279 Robert Haas, IBM

1280	Thomas Hardjono, M.I.T.
1281	ChengDong He, Huawei Technologies Co., Ltd.
1282	Steve He, Vormetric
1283	Kurt Heberlein, Hewlett-Packard
1284	Larry Hofer, Emulex Corporation
1285	Maryann Hondo, IBM
1286	Walt Hubis, NetApp
1287	Tim Hudson, Cryptsoft
1288	Jonas Iggbom, Venafi, Inc.
1289	Sitaram Inguva, American Express CCoE
1290	Jay Jacobs, Target Corporation
1291	Glen Jaquette, IBM
1292	Mahadev Karadiguddi, NetApp
1293	Greg Kazmierczak, Wave Systems Corp.
1294	Marc Kenig, SafeNet, Inc.
1295	Mark Knight, Thales e-Security
1296	Kathy Kriese, Symantec Corporation
1297	Mark Lambiase, SecureAuth
1298	John Leiseboer, Quintessence Labs
1299	Hal Lockhart, Oracle Corporation
1300	Robert Lockhart, Thales e-Security
1301	Anne Luk, Cryptsoft
1302	Sairam Manidi, Freescale
1303	Luther Martin, Voltage Security
1304	Neil McEvoy, iFOSSF
1305	Marina Milshtein, Individual
1306	Dale Moberg, Axway Software
1307	Jishnu Mukeri, Hewlett-Packard
1308	Bryan Olson, Hewlett-Packard
1309	John Peck, IBM
1310	Rob Philpott, EMC Corporation
1311	Denis Pochuev, SafeNet, Inc.
1312	Reid Poole, Venafi, Inc.
1313	Ajai Puri, SafeNet, Inc.
1314	Saravanan Ramalingam, Thales e-Security
1315	Peter Reed, SafeNet, Inc.
1316	Bruce Rich, IBM
1317	Christina Richards, American Express CCoE
1318	Warren Robbins, Dell
1319	Peter Robinson, EMC Corporation
1320	Scott Rotondo, Oracle
1321	Saikat Saha, SafeNet, Inc.
1322	Anil Saldhana, Red Hat
1323	Subhash Sankuratipati, NetApp
1324	Boris Schumperli, Cryptomathic
1325	Greg Singh, QuintessenceLabs
1326	David Smith, Venafi, Inc
1327	Brian Spector, Certivox
1328	Terence Spies, Voltage Security
1329	Deborah Steckroth, RouteOne LLC
1330	Michael Stevens, QuintessenceLabs
1331	Marcus Streets, Thales e-Security
1332	Satish Sundar, IBM
1333	Kiran Thota, VMware
1334	Somanchi Trinath, Freescale Semiconductor, Inc.
1335	Nathan Turajski, Thales e-Security

1336 Sean Turner, IECA, Inc.
1337 Paul Turner, Venafi, Inc.
1338 Rod Wideman, Quantum Corporation
1339 Steven Wierenga, Hewlett-Packard
1340 Jin Wong, QuintessenceLabs
1341 Sameer Yami, Thales e-Security
1342 Peter Yee, EMC Corporation
1343 Krishna Yellepeddy, IBM
1344 Catherine Ying, SafeNet, Inc.
1345 Tatu Ylonen, SSH Communications Security (Tectia Corp)
1346 Michael Yoder, Vormetric. Inc.
1347 Magda Zdunkiewicz, Cryptsoft
1348 Peter Zelechowski, Election Systems & Software
1349

1350 Appendix B. Revision History

Revision	Date	Editor	Changes Made
wd01	26-June-2013	Tim Hudson / Faisal Faruqui	Initial draft with updated conformance wording style. Updated test case style. Included test cases for 1.0, 1.1 and 1.2. Applied new OASIS template.
wd02	6-August-2013	Tim Hudson / Faisal Faruqui	Updated Test Cases based on July 2013 Interop
wd02a	24-October-2013	Tim Hudson	Editorial corrections to two typographical errors in the test cases in TC-71-{10,11,12}, TC-MDO-{1,2}.
pr01update	11-June-2014	Tim Hudson	Updated following Public Review

1351