

KMIP Symmetric Key Lifecycle Profile Version 1.0

Committee Specification Draft 02 / Public Review Draft 02

19 June 2014

Specification URIs

This version:

<http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/csprd02/kmip-sym-key-profile-v1.0-csprd02.doc> (Authoritative)

<http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/csprd02/kmip-sym-key-profile-v1.0-csprd02.html>

<http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/csprd02/kmip-sym-key-profile-v1.0-csprd02.pdf>

Previous version:

<http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/csprd01/kmip-sym-key-profile-v1.0-csprd01.doc> (Authoritative)

<http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/csprd01/kmip-sym-key-profile-v1.0-csprd01.html>

<http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/csprd01/kmip-sym-key-profile-v1.0-csprd01.pdf>

Latest version:

<http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/kmip-sym-key-profile-v1.0.doc>
(Authoritative)

<http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/kmip-sym-key-profile-v1.0.html>

<http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/kmip-sym-key-profile-v1.0.pdf>

Technical Committee:

OASIS Key Management Interoperability Protocol (KMIP) TC

Chairs:

Subhash Sankuratripati (Subhash.Sankuratripati@netapp.com), NetApp
Saikat Saha (saikat.saha@oracle.com), Oracle

Editors:

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

Robert Lockhart (Robert.Lockhart@thalesesec.com), Thales e-Security

Related work:

This specification is related to:

- *Key Management Interoperability Protocol Profiles Version 1.0*. Edited by Robert Griffin and Subhash Sankuratripati. 01 October 2010. OASIS Standard. <http://docs.oasis-open.org/kmip/profiles/v1.0/os/kmip-profiles-1.0-os.html>.
- *Key Management Interoperability Protocol Specification Version 1.1*. Edited by Robert Haas and Indra Fitzgerald. 24 January 2013. OASIS Standard. <http://docs.oasis-open.org/kmip/spec/v1.1/os/kmip-spec-v1.1-os.html>

- *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>.

Abstract:

Describes a profile for a KMIP server performing symmetric key lifecycle operations based on requests received from a KMIP client.

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.

Technical Committee members should send comments on this specification 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/>.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (<https://www.oasis-open.org/committees/kmip/ipr.php>).

Citation format:

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

[kmip-sym-key-v1.0]

KMIP Symmetric Key Lifecycle Profile Version 1.0. Edited by Tim Hudson and Robert Lockhart. 19 June 2014. OASIS Committee Specification Draft 02 / Public Review Draft 02.

<http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/csprd02/kmip-sym-key-profile-v1.0-csprd02.html>. Latest version: <http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/kmip-sym-key-profile-v1.0.html>.

Notices

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.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of [OASIS](#), the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <https://www.oasis-open.org/policies-guidelines/trademark> for above guidance.

Table of Contents

1	Introduction.....	5
1.1	Terminology.....	5
1.2	Normative References.....	5
2	Symmetric Key Lifecycle Profile.....	6
2.1	Authentication Suite.....	6
2.2	Symmetric Key Lifecycle - Client.....	6
2.3	Symmetric Key Lifecycle - Server.....	6
3	Symmetric Key Lifecycle Profile - Test Cases.....	8
3.1	Mandatory Test Cases KMIP v1.0.....	8
3.1.1	SKLC-M-1-10.....	8
3.1.2	SKLC-M-2-10.....	11
3.1.3	SKLC-M-3-10.....	18
3.2	Mandatory Test Cases KMIP v1.1.....	25
3.2.1	SKLC-M-1-11.....	25
3.2.2	SKLC-M-2-11.....	28
3.2.3	SKLC-M-3-11.....	35
3.3	Mandatory Test Cases KMIP v1.2.....	42
3.3.1	SKLC-M-1-12.....	42
3.3.2	SKLC-M-2-12.....	45
3.3.3	SKLC-M-3-12.....	52
3.4	Optional Test Cases KMIP v1.0.....	59
3.4.1	SKLC-O-1-10.....	59
3.5	Optional Test Cases KMIP v1.1.....	64
3.5.1	SKLC-O-1-11.....	64
3.6	Optional Test Cases KMIP v1.2.....	69
3.6.1	SKLC-O-1-12.....	69
4	Conformance.....	76
4.1	Symmetric Key Lifecycle Client KMIP v1.0 Profile Conformance.....	76
4.2	Symmetric Key Lifecycle Client KMIP v1.1 Profile Conformance.....	76
4.3	Symmetric Key Lifecycle Client KMIP v1.2 Profile Conformance.....	76
4.4	Symmetric Key Lifecycle Server KMIP v1.0 Profile Conformance.....	76
4.5	Symmetric Key Lifecycle Server KMIP v1.1 Profile Conformance.....	76
4.6	Symmetric Key Lifecycle Server KMIP v1.2 Profile Conformance.....	76
4.7	Permitted Test Case Variations.....	76
4.7.1	Variable Items.....	77
4.7.2	Variable behavior.....	78
Appendix A.	Acknowledgments.....	79
Appendix B.	KMIP Specification Cross Reference.....	82
Appendix C.	Revision History.....	87

1 Introduction

For normative definition of the elements of KMIP see the [KMIP Specification](#) [KMIP-SPEC] and the [KMIP Profiles](#) [KMIP-PROF].

This profile defines the necessary KMIP functionality that a KMIP server conforming to this profile SHALL support in order to interoperate in conformance with this profile.

1.1 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

1.2 Normative References

- [RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- [KMIP-ENCODE] *KMIP Additional Message Encodings Version 1.0*.
[URL](#)
Candidate OASIS Standard 01. DD MMM YYYY.
- [KMIP-SPEC] One or more of [KMIP-SPEC-1_0], [KMIP-SPEC-1_1], [KMIP-SPEC-1_2]
- [KMIP-SPEC-1_0] *Key Management Interoperability Protocol Specification Version 1.0*
<http://docs.oasis-open.org/kmip/spec/v1.0/os/kmip-spec-1.0-os.doc>
OASIS Standard, October 2010.
- [KMIP-SPEC-1_1] *Key Management Interoperability Protocol Specification Version 1.1*.
<http://docs.oasis-open.org/kmip/spec/v1.1/os/kmip-spec-v1.1-os.doc>
OASIS Standard. 24 January 2013.
- [KMIP-SPEC-1_2] *Key Management Interoperability Protocol Specification Version 1.2*.
[URL](#)
Candidate OASIS Standard 01. DD MMM YYYY.
- [KMIP-PROF] One or more of [KMIP-PROF-1_0], [KMIP-PROF-1_1], [KMIP-PROF-1_2]
- [KMIP-PROF-1_0] *Key Management Interoperability Protocol Profiles Version 1.0*. <http://docs.oasis-open.org/kmip/profiles/v1.0/os/kmip-profiles-1.0-os.doc>
OASIS Standard. 1 October 2010.
- [KMIP-PROF-1_1] *Key Management Interoperability Protocol Profiles Version 1.1*.
<http://docs.oasis-open.org/kmip/profiles/v1.1/os/kmip-profiles-v1.1-os.doc>
OASIS Standard 01. 24 January 2013.
- [KMIP-PROF-1_2] *Key Management Interoperability Protocol Profiles Version 1.2*.
[URL](#)
Candidate OASIS Standard 01. DD MMM YYYY.
- Committee Note Draft, DD MMM YYYY

37 2 Symmetric Key Lifecycle Profile

38 The Symmetric Key Lifecycle Profile is a KMIP server performing symmetric key lifecycle operations
39 based on requests received from a KMIP client.

40 2.1 Authentication Suite

41 Implementations conformant to this profile SHALL support at least one of the Authentication Suites
42 defined within section 3 of [KMIP-PROF]. The establishment of the trust relationship between the KMIP
43 client and the KMIP server is the same as the defined base profiles.

44 2.2 Symmetric Key Lifecycle - Client

45 KMIP clients conformant to this profile under [KMIP-SPEC-1_0]:

46 1. SHALL conform to the [KMIP-SPEC-1_0]

47 KMIP clients conformant to this profile under [KMIP-SPEC-1_1]:

48 2. SHALL conform to the *Baseline Client Clause* (section 5.12) of [KMIP-PROF-1_1]

49 KMIP clients conformant to this profile under [KMIP-SPEC-1_2]:

50 3. SHALL conform to the *Baseline Client* (section 5.2) of [KMIP-PROF-1_2]

51 KMIP clients conformant to this profile:

52 4. MAY support any clause within [KMIP-SPEC] provided it does not conflict with any other clause
53 within this section 2.2

54 5. MAY support extensions outside the scope of this standard (e.g., vendor extensions,
55 conformance clauses) that do not contradict any KMIP requirements.

56 2.3 Symmetric Key Lifecycle - Server

57 KMIP servers conformant to this profile under [KMIP-SPEC-1_0]:

58 1. SHALL conform to the [KMIP-SPEC-1_0]

59 KMIP clients conformant to this profile under [KMIP-SPEC-1_1]:

60 2. SHALL conform to the *Baseline Server Clause* of [KMIP-PROF-1_1]

61 KMIP clients conformant to this profile under [KMIP-SPEC-1_2]:

62 3. SHALL conform to the *Baseline Server* of [KMIP-PROF-1_2]

63 KMIP servers conformant to this profile:

64 4. SHALL conform to the KMIP Baseline Server profile in [KMIP-PROF] and [KMIP-SPEC] and

65 5. SHALL support the following *Objects* [KMIP-SPEC]

66 a. *Symmetric Key* [KMIP-SPEC]

67 b. *Key Format Type* [KMIP-SPEC]

68 6. SHALL support the following *Attributes* [KMIP-SPEC]

69 a. *Cryptographic Algorithm* [KMIP-SPEC]

70 b. *Object Type* [KMIP-SPEC]

71 c. *Process Start Date* [KMIP-SPEC]

72 d. *Protect Stop Date* [KMIP-SPEC]

73 7. SHALL support the following *Client-to-Server* [KMIP-SPEC] operations:

74 a. *Create* [KMIP-SPEC]

- 75 8. SHALL support the following *Message Encoding* [KMIP-SPEC]:
76 a. *Cryptographic Algorithm* [KMIP-SPEC] with values:
77 i. 3DES
78 ii. AES
79 b. *Object Type* [KMIP-SPEC] with value:
80 iii. Symmetric Key
81 c. *Key Format Type* [KMIP-SPEC] with value:
82 iv. Raw
83 v. Transparent Symmetric Key
84 9. MAY support any clause within [KMIP-SPEC] provided it does not conflict with any other clause
85 within this section 2.3
86 10. MAY support extensions outside the scope of this standard (e.g., vendor extensions,
87 conformance clauses) that do not contradict any KMIP requirements.

88 3 Symmetric Key Lifecycle Profile - Test Cases

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

93 Each test case has a unique label (the section name) which includes indication of mandatory (-M-) or
94 optional (-O-) status and the protocol version major and minor numbers as part of the identifier.

95 The test cases may depend on a specific configuration of a KMIP client and server being configured in a
96 manner consistent with the test case assumptions.

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

100 Note: the values for the returned items and the custom attributes are illustrative. Actual values from a real
101 client or server system may vary as specified in section 4.7.

102 3.1 Mandatory Test Cases KMIP v1.0

103 3.1.1 SKLC-M-1-10

104 Create, GetAttributes, Destroy

```
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="256"/>
0024         </Attribute>
0025         <Attribute>
0026           <AttributeName type="TextString" value="Cryptographic
0027 Usage Mask"/>
0028           <AttributeValue type="Integer" value="Encrypt Decrypt"/>
0029         </Attribute>
0030         <Attribute>
0031           <AttributeName type="TextString" value="Name"/>
0032           <AttributeValue type="TextString" value="Name"/>
0033         </Attribute>
0034       </TemplateAttribute>
0035     </RequestPayload>
0036   </BatchItem>
0037 </BatchItem>
0038 </RequestMessage>
```


0029	<NameValue type="TextString" value="SKLC-M-1-10"/>
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="2012-04-27T08:12:24+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>
	<i># TIME 1</i>
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="GetAttributes"/>
0065	<RequestPayload>
0066	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0067	<AttributeName type="TextString" value="State"/>
0068	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0069	<AttributeName type="TextString" value="Unique Identifier"/>
0070	<AttributeName type="TextString" value="Object Type"/>
0071	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0072	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0073	<AttributeName type="TextString" value="Digest"/>
0074	<AttributeName type="TextString" value="Initial Date"/>
0075	<AttributeName type="TextString" value="Last Change Date"/>
0076	<AttributeName type="TextString" value="Activation Date"/>
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="2012-04-27T08:12:24+00:00"/>
0087     <BatchCount type="Integer" value="1"/>
0088   </ResponseHeader>
0089   <BatchItem>
0090     <Operation type="Enumeration" value="GetAttributes"/>
0091     <ResultStatus type="Enumeration" value="Success"/>
0092     <ResponsePayload>
0093       <UniqueIdentifier type="TextString"
0094 value="$UNIQUE_IDENTIFIER_0"/>
0095       <Attribute>
0096         <AttributeName type="TextString" value="State"/>
0097         <AttributeValue type="Enumeration" value="PreActive"/>
0098       </Attribute>
0099       <Attribute>
0100         <AttributeName type="TextString" value="Cryptographic Usage
0101 Mask"/>
0102         <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0103       </Attribute>
0104       <Attribute>
0105         <AttributeName type="TextString" value="Unique Identifier"/>
0106         <AttributeValue type="TextString"
0107 value="$UNIQUE_IDENTIFIER_0"/>
0108       </Attribute>
0109       <Attribute>
0110         <AttributeName type="TextString" value="Object Type"/>
0111         <AttributeValue type="Enumeration" value="SymmetricKey"/>
0112       </Attribute>
0113       <Attribute>
0114         <AttributeName type="TextString" value="Cryptographic
0115 Algorithm"/>
0116         <AttributeValue type="Enumeration" value="AES"/>
0117       </Attribute>
0118       <Attribute>
0119         <AttributeName type="TextString" value="Cryptographic
0120 Length"/>
0121         <AttributeValue type="Integer" value="256"/>
0122       </Attribute>
0123       <Attribute>
0124         <AttributeName type="TextString" value="Digest"/>
0125         <AttributeValue>
0126           <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0127           <DigestValue type="ByteString"
0128 value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046a1b931fdaed73591
0129 f29"/>
0130         </AttributeValue>
0131       </Attribute>
0132       <Attribute>
0133         <AttributeName type="TextString" value="Initial Date"/>
0134         <AttributeValue type="DateTime" value="2013-01-
0135 10T23:33:21+00:00"/>
0136       </Attribute>
0137     </ResponsePayload>
0138   </BatchItem>
0139 </ResponseMessage>

```

0130	<AttributeName type="TextString" value="Last Change Date"/>
0131	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0132	</Attribute>
0133	</ResponsePayload>
0134	</BatchItem>
0135	</ResponseMessage>
# TIME 2	
0136	<RequestMessage>
0137	<RequestHeader>
0138	<ProtocolVersion>
0139	<ProtocolVersionMajor type="Integer" value="1"/>
0140	<ProtocolVersionMinor type="Integer" value="0"/>
0141	</ProtocolVersion>
0142	<BatchCount type="Integer" value="1"/>
0143	</RequestHeader>
0144	<BatchItem>
0145	<Operation type="Enumeration" value="Destroy"/>
0146	<RequestPayload>
0147	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0148	</RequestPayload>
0149	</BatchItem>
0150	</RequestMessage>
0151	<ResponseMessage>
0152	<ResponseHeader>
0153	<ProtocolVersion>
0154	<ProtocolVersionMajor type="Integer" value="1"/>
0155	<ProtocolVersionMinor type="Integer" value="0"/>
0156	</ProtocolVersion>
0157	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0158	<BatchCount type="Integer" value="1"/>
0159	</ResponseHeader>
0160	<BatchItem>
0161	<Operation type="Enumeration" value="Destroy"/>
0162	<ResultStatus type="Enumeration" value="Success"/>
0163	<ResponsePayload>
0164	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0165	</ResponsePayload>
0166	</BatchItem>
0167	</ResponseMessage>

105

106 3.1.2 SKLC-M-2-10

107 Create, GetAttributes, Activate, GetAttributes, Destroy, Revoke, GetAttributes, Destroy

# 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="256"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0024	<AttributeValue type="Integer" value="Encrypt Decrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="SKLC-M-2-10"/>
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="2012-04-27T08:12:24+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="0"/>
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="$UNIQUE_IDENTIFIER_0"/>
0067     <AttributeName type="TextString" value="State"/>
0068     <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0069     <AttributeName type="TextString" value="Unique Identifier"/>
0070     <AttributeName type="TextString" value="Object Type"/>
0071     <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0072     <AttributeName type="TextString" value="Cryptographic
Length"/>
0073     <AttributeName type="TextString" value="Digest"/>
0074     <AttributeName type="TextString" value="Initial Date"/>
0075     <AttributeName type="TextString" value="Last Change Date"/>
0076   </RequestPayload>
0077 </BatchItem>
0078 </RequestMessage>
0079 <ResponseMessage>
0080 <ResponseHeader>
0081   <ProtocolVersion>
0082     <ProtocolVersionMajor type="Integer" value="1"/>
0083     <ProtocolVersionMinor type="Integer" value="0"/>
0084   </ProtocolVersion>
0085   <TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0086   <BatchCount type="Integer" value="1"/>
0087 </ResponseHeader>
0088 <BatchItem>
0089   <Operation type="Enumeration" value="GetAttributes"/>
0090   <ResultStatus type="Enumeration" value="Success"/>
0091   <ResponsePayload>
0092     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0093     <Attribute>
0094       <AttributeName type="TextString" value="State"/>
0095       <AttributeValue type="Enumeration" value="PreActive"/>
0096     </Attribute>
0097     <Attribute>
0098       <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0099       <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0100     </Attribute>
0101     <Attribute>
0102       <AttributeName type="TextString" value="Unique Identifier"/>
0103       <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0104     </Attribute>
0105     <Attribute>
0106       <AttributeName type="TextString" value="Object Type"/>
0107       <AttributeValue type="Enumeration" value="SymmetricKey"/>
0108     </Attribute>
0109     <Attribute>
0110       <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0111       <AttributeValue type="Enumeration" value="AES"/>

```

0112	</Attribute>
0113	<Attribute>
0114	<AttributeName type="TextString" value="Cryptographic Length"/>
0115	<AttributeValue type="Integer" value="256"/>
0116	</Attribute>
0117	<Attribute>
0118	<AttributeName type="TextString" value="Digest"/>
0119	<AttributeValue>
0120	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0121	<DigestValue type="ByteString" value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046a1b931fdaed73591f29"/>
0122	</AttributeValue>
0123	</Attribute>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Initial Date"/>
0126	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0127	</Attribute>
0128	<Attribute>
0129	<AttributeName type="TextString" value="Last Change Date"/>
0130	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0131	</Attribute>
0132	</ResponsePayload>
0133	</BatchItem>
0134	</ResponseMessage>
0135	<i># TIME 2</i> <RequestMessage>
0136	<RequestHeader>
0137	<ProtocolVersion>
0138	<ProtocolVersionMajor type="Integer" value="1"/>
0139	<ProtocolVersionMinor type="Integer" value="0"/>
0140	</ProtocolVersion>
0141	<BatchCount type="Integer" value="1"/>
0142	</RequestHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="Activate"/>
0145	<RequestPayload>
0146	<UniqueIdentifier type="TextString" 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="0"/>
0155	</ProtocolVersion>
0156	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0157	<BatchCount type="Integer" value="1"/>
0158	</ResponseHeader>
0159	<BatchItem>
0160	<Operation type="Enumeration" value="Activate"/>
0161	<ResultStatus type="Enumeration" value="Success"/>
0162	<ResponsePayload>

0163	<UniqueIdentifier type="TextString"
0164	value="\$UNIQUE_IDENTIFIER_0"/>
0165	</ResponsePayload>
0166	</BatchItem>
0167	</ResponseMessage>
	# TIME 3
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="GetAttributes"/>
0177	<RequestPayload>
0178	<UniqueIdentifier type="TextString"
0179	value="\$UNIQUE_IDENTIFIER_0"/>
0180	<AttributeName type="TextString" value="State"/>
0181	<AttributeName type="TextString" value="Activation Date"/>
0182	<AttributeName type="TextString" value="Deactivation Date"/>
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="2012-04-27T08:12:24+00:00"/>
0193	<BatchCount type="Integer" value="1"/>
0194	</ResponseHeader>
0195	<BatchItem>
0196	<Operation type="Enumeration" value="GetAttributes"/>
0197	<ResultStatus type="Enumeration" value="Success"/>
0198	<ResponsePayload>
0199	<UniqueIdentifier type="TextString"
0200	value="\$UNIQUE_IDENTIFIER_0"/>
0201	<Attribute>
0202	<AttributeName type="TextString" value="State"/>
0203	<AttributeValue type="Enumeration" value="Active"/>
0204	</Attribute>
0205	<Attribute>
0206	<AttributeName type="TextString" value="Activation Date"/>
0207	<AttributeValue type="DateTime" value="2013-01-10T23:36:01+00:00"/>
0208	</Attribute>
0209	</ResponsePayload>
0210	</BatchItem>
0211	</ResponseMessage>
	# TIME 4
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="Destroy"/>
0220	<RequestPayload>
0221	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
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="2012-04-27T08:12:25+00:00"/>
0232	<BatchCount type="Integer" value="1"/>
0233	</ResponseHeader>
0234	<BatchItem>
0235	<Operation type="Enumeration" value="Destroy"/>
0236	<ResultStatus type="Enumeration" value="OperationFailed"/>
0237	<ResultReason type="Enumeration" value="PermissionDenied"/>
0238	<ResultMessage type="TextString" value="DENIED"/>
0239	</BatchItem>
0240	</ResponseMessage>
	# TIME 5
0241	<RequestMessage>
0242	<RequestHeader>
0243	<ProtocolVersion>
0244	<ProtocolVersionMajor type="Integer" value="1"/>
0245	<ProtocolVersionMinor type="Integer" value="0"/>
0246	</ProtocolVersion>
0247	<BatchCount type="Integer" value="1"/>
0248	</RequestHeader>
0249	<BatchItem>
0250	<Operation type="Enumeration" value="Revoke"/>
0251	<RequestPayload>
0252	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0253	<RevocationReason>
0254	<RevocationReasonCode type="Enumeration"
	value="KeyCompromise"/>
0255	</RevocationReason>
0256	<CompromiseOccurrenceDate type="DateTime" value="1970-01-
	01T00:00:06+00:00"/>
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="2012-04-27T08:12:24+00:00"/>
0267	<BatchCount type="Integer" value="1"/>

0268	</ResponseHeader>
0269	<BatchItem>
0270	<Operation type="Enumeration" value="Revoke"/>
0271	<ResultStatus type="Enumeration" value="Success"/>
0272	<ResponsePayload>
0273	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0274	</ResponsePayload>
0275	</BatchItem>
0276	</ResponseMessage>
# TIME 6	
0277	<RequestMessage>
0278	<RequestHeader>
0279	<ProtocolVersion>
0280	<ProtocolVersionMajor type="Integer" value="1"/>
0281	<ProtocolVersionMinor type="Integer" value="0"/>
0282	</ProtocolVersion>
0283	<BatchCount type="Integer" value="1"/>
0284	</RequestHeader>
0285	<BatchItem>
0286	<Operation type="Enumeration" value="GetAttributes"/>
0287	<RequestPayload>
0288	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0289	<AttributeName type="TextString" value="State"/>
0290	</RequestPayload>
0291	</BatchItem>
0292	</RequestMessage>
0293	<ResponseMessage>
0294	<ResponseHeader>
0295	<ProtocolVersion>
0296	<ProtocolVersionMajor type="Integer" value="1"/>
0297	<ProtocolVersionMinor type="Integer" value="0"/>
0298	</ProtocolVersion>
0299	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0300	<BatchCount type="Integer" value="1"/>
0301	</ResponseHeader>
0302	<BatchItem>
0303	<Operation type="Enumeration" value="GetAttributes"/>
0304	<ResultStatus type="Enumeration" value="Success"/>
0305	<ResponsePayload>
0306	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0307	<Attribute>
0308	<AttributeName type="TextString" value="State"/>
0309	<AttributeValue type="Enumeration" value="Compromised"/>
0310	</Attribute>
0311	</ResponsePayload>
0312	</BatchItem>
0313	</ResponseMessage>
# TIME 7	
0314	<RequestMessage>
0315	<RequestHeader>
0316	<ProtocolVersion>
0317	<ProtocolVersionMajor type="Integer" value="1"/>
0318	<ProtocolVersionMinor type="Integer" value="0"/>
0319	</ProtocolVersion>
0320	<BatchCount type="Integer" value="1"/>

0321	</RequestHeader>
0322	<BatchItem>
0323	<Operation type="Enumeration" value="Destroy"/>
0324	<RequestPayload>
0325	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0326	</RequestPayload>
0327	</BatchItem>
0328	</RequestMessage>
0329	<ResponseMessage>
0330	<ResponseHeader>
0331	<ProtocolVersion>
0332	<ProtocolVersionMajor type="Integer" value="1"/>
0333	<ProtocolVersionMinor type="Integer" value="0"/>
0334	</ProtocolVersion>
0335	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0336	<BatchCount type="Integer" value="1"/>
0337	</ResponseHeader>
0338	<BatchItem>
0339	<Operation type="Enumeration" value="Destroy"/>
0340	<ResultStatus type="Enumeration" value="Success"/>
0341	<ResponsePayload>
0342	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0343	</ResponsePayload>
0344	</BatchItem>
0345	</ResponseMessage>

108

109 3.1.3 SKLC-M-3-10

110 Create, GetAttributes, Activate, GetAttributes, Destroy, Revoke, GetAttributes, Destroy

	# 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="256"/>
0021	</Attribute>
0022	</Attribute>

0023	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0024	<AttributeValue type="Integer" value="Encrypt Decrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="SKLC-M-3-10"/>
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="2012-04-27T08:12:24+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="0"/>
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	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0069	<AttributeName type="TextString" value="Unique Identifier"/>
0070	<AttributeName type="TextString" value="Object Type"/>
0071	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0072	<AttributeName type="TextString" value="Cryptographic Length"/>

0073	<AttributeName type="TextString" value="Digest"/>
0074	<AttributeName type="TextString" value="Initial Date"/>
0075	<AttributeName type="TextString" value="Last Change Date"/>
0076	</RequestPayload>
0077	</BatchItem>
0078	</RequestMessage>
0079	<ResponseMessage>
0080	<ResponseHeader>
0081	<ProtocolVersion>
0082	<ProtocolVersionMajor type="Integer" value="1"/>
0083	<ProtocolVersionMinor type="Integer" value="0"/>
0084	</ProtocolVersion>
0085	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0086	<BatchCount type="Integer" value="1"/>
0087	</ResponseHeader>
0088	<BatchItem>
0089	<Operation type="Enumeration" value="GetAttributes"/>
0090	<ResultStatus type="Enumeration" value="Success"/>
0091	<ResponsePayload>
0092	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0093	<Attribute>
0094	<AttributeName type="TextString" value="State"/>
0095	<AttributeValue type="Enumeration" value="PreActive"/>
0096	</Attribute>
0097	<Attribute>
0098	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0099	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0100	</Attribute>
0101	<Attribute>
0102	<AttributeName type="TextString" value="Unique Identifier"/>
0103	<AttributeValue type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0104	</Attribute>
0105	<Attribute>
0106	<AttributeName type="TextString" value="Object Type"/>
0107	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0108	</Attribute>
0109	<Attribute>
0110	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0111	<AttributeValue type="Enumeration" value="AES"/>
0112	</Attribute>
0113	<Attribute>
0114	<AttributeName type="TextString" value="Cryptographic Length"/>
0115	<AttributeValue type="Integer" value="256"/>
0116	</Attribute>
0117	<Attribute>
0118	<AttributeName type="TextString" value="Digest"/>
0119	<AttributeValue>
0120	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0121	<DigestValue type="ByteString" value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046a1b931fdaed73591f29"/>
0122	</AttributeValue>
0123	</Attribute>

0124	<Attribute>
0125	<AttributeName type="TextString" value="Initial Date"/>
0126	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0127	</Attribute>
0128	<Attribute>
0129	<AttributeName type="TextString" value="Last Change Date"/>
0130	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0131	</Attribute>
0132	</ResponsePayload>
0133	</BatchItem>
0134	</ResponseMessage>
# TIME 2	
0135	<RequestMessage>
0136	<RequestHeader>
0137	<ProtocolVersion>
0138	<ProtocolVersionMajor type="Integer" value="1"/>
0139	<ProtocolVersionMinor type="Integer" value="0"/>
0140	</ProtocolVersion>
0141	<BatchCount type="Integer" value="1"/>
0142	</RequestHeader>
0143	<BatchItem>
0144	<Operation type="Enumeration" value="Activate"/>
0145	<RequestPayload>
0146	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0147	</RequestPayload>
0148	</BatchItem>
0149	</RequestMessage>
# TIME 3	
0150	<ResponseMessage>
0151	<ResponseHeader>
0152	<ProtocolVersion>
0153	<ProtocolVersionMajor type="Integer" value="1"/>
0154	<ProtocolVersionMinor type="Integer" value="0"/>
0155	</ProtocolVersion>
0156	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0157	<BatchCount type="Integer" value="1"/>
0158	</ResponseHeader>
0159	<BatchItem>
0160	<Operation type="Enumeration" value="Activate"/>
0161	<ResultStatus type="Enumeration" value="Success"/>
0162	<ResponsePayload>
0163	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0164	</ResponsePayload>
0165	</BatchItem>
0166	</ResponseMessage>
# TIME 3	
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="GetAttributes"/>
0177	<RequestPayload>
0178	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0179	<AttributeName type="TextString" value="State"/>
0180	<AttributeName type="TextString" value="Activation Date"/>
0181	<AttributeName type="TextString" value="Deactivation Date"/>
0182	</RequestPayload>
0183	</BatchItem>
0184	</RequestMessage>
0185	<ResponseMessage>
0186	<ResponseHeader>
0187	<ProtocolVersion>
0188	<ProtocolVersionMajor type="Integer" value="1"/>
0189	<ProtocolVersionMinor type="Integer" value="0"/>
0190	</ProtocolVersion>
0191	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0192	<BatchCount type="Integer" value="1"/>
0193	</ResponseHeader>
0194	<BatchItem>
0195	<Operation type="Enumeration" value="GetAttributes"/>
0196	<ResultStatus type="Enumeration" value="Success"/>
0197	<ResponsePayload>
0198	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0199	<Attribute>
0200	<AttributeName type="TextString" value="State"/>
0201	<AttributeValue type="Enumeration" value="Active"/>
0202	</Attribute>
0203	<Attribute>
0204	<AttributeName type="TextString" value="Activation Date"/>
0205	<AttributeValue type="DateTime" value="2013-01-
	10T23:36:01+00:00"/>
0206	</Attribute>
0207	</ResponsePayload>
0208	</BatchItem>
0209	</ResponseMessage>
	# TIME 4
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="ModifyAttribute"/>
0220	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0221	<RequestPayload>
0222	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0223	<Attribute>
0224	<AttributeName type="TextString" value="Activation Date"/>
0225	<AttributeValue type="DateTime" value="\$NOW"/>
0226	</Attribute>
0227	</RequestPayload>
0228	</BatchItem>

0229	</RequestMessage>
0230	<ResponseMessage>
0231	<ResponseHeader>
0232	<ProtocolVersion>
0233	<ProtocolVersionMajor type="Integer" value="1"/>
0234	<ProtocolVersionMinor type="Integer" value="0"/>
0235	</ProtocolVersion>
0236	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0237	<BatchCount type="Integer" value="1"/>
0238	</ResponseHeader>
0239	<BatchItem>
0240	<Operation type="Enumeration" value="ModifyAttribute"/>
0241	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0242	<ResultStatus type="Enumeration" value="OperationFailed"/>
0243	<ResultReason type="Enumeration" value="PermissionDenied"/>
0244	<ResultMessage type="TextString" value="DENIED"/>
0245	</BatchItem>
0246	</ResponseMessage>
	# TIME 5
0247	<RequestMessage>
0248	<RequestHeader>
0249	<ProtocolVersion>
0250	<ProtocolVersionMajor type="Integer" value="1"/>
0251	<ProtocolVersionMinor type="Integer" value="0"/>
0252	</ProtocolVersion>
0253	<BatchCount type="Integer" value="1"/>
0254	</RequestHeader>
0255	<BatchItem>
0256	<Operation type="Enumeration" value="Revoke"/>
0257	<RequestPayload>
0258	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0259	<RevocationReason>
0260	<RevocationReasonCode type="Enumeration" value="KeyCompromise"/>
0261	</RevocationReason>
0262	<CompromiseOccurrenceDate type="DateTime" value="1970-01-01T00:00:06+00:00"/>
0263	</RequestPayload>
0264	</BatchItem>
0265	</RequestMessage>
0266	<ResponseMessage>
0267	<ResponseHeader>
0268	<ProtocolVersion>
0269	<ProtocolVersionMajor type="Integer" value="1"/>
0270	<ProtocolVersionMinor type="Integer" value="0"/>
0271	</ProtocolVersion>
0272	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0273	<BatchCount type="Integer" value="1"/>
0274	</ResponseHeader>
0275	<BatchItem>
0276	<Operation type="Enumeration" value="Revoke"/>
0277	<ResultStatus type="Enumeration" value="Success"/>
0278	<ResponsePayload>
0279	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0280	</ResponsePayload>
0281	</BatchItem>

0282	</ResponseMessage>
	# TIME 6
0283	<RequestMessage>
0284	<RequestHeader>
0285	<ProtocolVersion>
0286	<ProtocolVersionMajor type="Integer" value="1"/>
0287	<ProtocolVersionMinor type="Integer" value="0"/>
0288	</ProtocolVersion>
0289	<BatchCount type="Integer" value="1"/>
0290	</RequestHeader>
0291	<BatchItem>
0292	<Operation type="Enumeration" value="GetAttributes"/>
0293	<RequestPayload>
0294	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0295	<AttributeName type="TextString" value="State"/>
0296	</RequestPayload>
0297	</BatchItem>
0298	</RequestMessage>
0299	<ResponseMessage>
0300	<ResponseHeader>
0301	<ProtocolVersion>
0302	<ProtocolVersionMajor type="Integer" value="1"/>
0303	<ProtocolVersionMinor type="Integer" value="0"/>
0304	</ProtocolVersion>
0305	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0306	<BatchCount type="Integer" value="1"/>
0307	</ResponseHeader>
0308	<BatchItem>
0309	<Operation type="Enumeration" value="GetAttributes"/>
0310	<ResultStatus type="Enumeration" value="Success"/>
0311	<ResponsePayload>
0312	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0313	<Attribute>
0314	<AttributeName type="TextString" value="State"/>
0315	<AttributeValue type="Enumeration" value="Compromised"/>
0316	</Attribute>
0317	</ResponsePayload>
0318	</BatchItem>
0319	</ResponseMessage>
	# TIME 7
0320	<RequestMessage>
0321	<RequestHeader>
0322	<ProtocolVersion>
0323	<ProtocolVersionMajor type="Integer" value="1"/>
0324	<ProtocolVersionMinor type="Integer" value="0"/>
0325	</ProtocolVersion>
0326	<BatchCount type="Integer" value="1"/>
0327	</RequestHeader>
0328	<BatchItem>
0329	<Operation type="Enumeration" value="Destroy"/>
0330	<RequestPayload>
0331	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0332	</RequestPayload>
0333	</BatchItem>
0334	</RequestMessage>


```

0335 <ResponseMessage>
0336   <ResponseHeader>
0337     <ProtocolVersion>
0338       <ProtocolVersionMajor type="Integer" value="1"/>
0339       <ProtocolVersionMinor type="Integer" value="0"/>
0340     </ProtocolVersion>
0341     <TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0342     <BatchCount type="Integer" value="1"/>
0343   </ResponseHeader>
0344   <BatchItem>
0345     <Operation type="Enumeration" value="Destroy"/>
0346     <ResultStatus type="Enumeration" value="Success"/>
0347     <ResponsePayload>
0348       <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0349     </ResponsePayload>
0350   </BatchItem>
0351 </ResponseMessage>

```

111

112 3.2 Mandatory Test Cases KMIP v1.1

113 3.2.1 SKLC-M-1-11

114 Create, GetAttributes, 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="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="Encrypt Decrypt"/>
0025         </Attribute>
0026         <Attribute>
0027           <AttributeName type="TextString" value="Name"/>
0028           <AttributeValue>

```

0029	<NameValue type="TextString" value="SKLC-M-1-11"/>
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="2012-04-27T08:12:24+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="GetAttributes"/>
0065	<RequestPayload>
0066	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0067	<AttributeName type="TextString" value="State"/>
0068	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0069	<AttributeName type="TextString" value="Unique Identifier"/>
0070	<AttributeName type="TextString" value="Object Type"/>
0071	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0072	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0073	<AttributeName type="TextString" value="Digest"/>
0074	<AttributeName type="TextString" value="Initial Date"/>
0075	<AttributeName type="TextString" value="Last Change Date"/>
0076	<AttributeName type="TextString" value="Activation Date"/>
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="2012-04-27T08:12:24+00:00"/>
0087     <BatchCount type="Integer" value="1"/>
0088   </ResponseHeader>
0089   <BatchItem>
0090     <Operation type="Enumeration" value="GetAttributes"/>
0091     <ResultStatus type="Enumeration" value="Success"/>
0092     <ResponsePayload>
0093       <UniqueIdentifier type="TextString"
0094 value="$UNIQUE_IDENTIFIER_0"/>
0095       <Attribute>
0096         <AttributeName type="TextString" value="State"/>
0097         <AttributeValue type="Enumeration" value="PreActive"/>
0098       </Attribute>
0099       <Attribute>
0100         <AttributeName type="TextString" value="Cryptographic Usage
0101 Mask"/>
0102         <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0103       </Attribute>
0104       <Attribute>
0105         <AttributeName type="TextString" value="Unique Identifier"/>
0106         <AttributeValue type="TextString"
0107 value="$UNIQUE_IDENTIFIER_0"/>
0108       </Attribute>
0109       <Attribute>
0110         <AttributeName type="TextString" value="Object Type"/>
0111         <AttributeValue type="Enumeration" value="SymmetricKey"/>
0112       </Attribute>
0113       <Attribute>
0114         <AttributeName type="TextString" value="Cryptographic
0115 Algorithm"/>
0116         <AttributeValue type="Enumeration" value="AES"/>
0117       </Attribute>
0118       <Attribute>
0119         <AttributeName type="TextString" value="Cryptographic
0120 Length"/>
0121         <AttributeValue type="Integer" value="256"/>
0122       </Attribute>
0123       <Attribute>
0124         <AttributeName type="TextString" value="Digest"/>
0125         <AttributeValue>
0126           <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0127           <DigestValue type="ByteString"
0128 value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046a1b931fdaed73591
0129 f29"/>
0130         </AttributeValue>
0131       </Attribute>
0132       <Attribute>
0133         <AttributeName type="TextString" value="Initial Date"/>
0134         <AttributeValue type="DateTime" value="2013-01-
0135 10T23:33:21+00:00"/>
0136       </Attribute>

```

0130	<Attribute>
0131	<AttributeName type="TextString" value="Last Change Date"/>
0132	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0133	</Attribute>
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="Destroy"/>
0147	<RequestPayload>
0148	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0149	</RequestPayload>
0150	</BatchItem>
0151	</RequestMessage>
0152	<ResponseMessage>
0153	<ResponseHeader>
0154	<ProtocolVersion>
0155	<ProtocolVersionMajor type="Integer" value="1"/>
0156	<ProtocolVersionMinor type="Integer" value="1"/>
0157	</ProtocolVersion>
0158	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0159	<BatchCount type="Integer" value="1"/>
0160	</ResponseHeader>
0161	<BatchItem>
0162	<Operation type="Enumeration" value="Destroy"/>
0163	<ResultStatus type="Enumeration" value="Success"/>
0164	<ResponsePayload>
0165	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0166	</ResponsePayload>
0167	</BatchItem>
0168	</ResponseMessage>

115

116 3.2.2 SKLC-M-2-11

117 Create, GetAttributes, Activate, GetAttributes, Destroy, Revoke, GetAttributes, 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="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="Encrypt Decrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="SKLC-M-2-11"/>
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="2012-04-27T08:12:24+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="GetAttributes"/>
0065         <RequestPayload>
0066             <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0067             <AttributeName type="TextString" value="State"/>
0068             <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0069             <AttributeName type="TextString" value="Unique Identifier"/>
0070             <AttributeName type="TextString" value="Object Type"/>
0071             <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0072             <AttributeName type="TextString" value="Cryptographic
Length"/>
0073             <AttributeName type="TextString" value="Digest"/>
0074             <AttributeName type="TextString" value="Initial Date"/>
0075             <AttributeName type="TextString" value="Last Change Date"/>
0076         </RequestPayload>
0077     </BatchItem>
0078 </RequestMessage>
0079 <ResponseMessage>
0080     <ResponseHeader>
0081         <ProtocolVersion>
0082             <ProtocolVersionMajor type="Integer" value="1"/>
0083             <ProtocolVersionMinor type="Integer" value="1"/>
0084         </ProtocolVersion>
0085         <TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0086         <BatchCount type="Integer" value="1"/>
0087     </ResponseHeader>
0088     <BatchItem>
0089         <Operation type="Enumeration" value="GetAttributes"/>
0090         <ResultStatus type="Enumeration" value="Success"/>
0091         <ResponsePayload>
0092             <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0093             <Attribute>
0094                 <AttributeName type="TextString" value="State"/>
0095                 <AttributeValue type="Enumeration" value="PreActive"/>
0096             </Attribute>
0097             <Attribute>
0098                 <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0099                 <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0100             </Attribute>
0101             <Attribute>
0102                 <AttributeName type="TextString" value="Unique Identifier"/>
0103                 <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0104             </Attribute>
0105             <Attribute>
0106                 <AttributeName type="TextString" value="Object Type"/>
0107                 <AttributeValue type="Enumeration" value="SymmetricKey"/>
0108             </Attribute>
0109             <Attribute>
0110                 <AttributeName type="TextString" value="Cryptographic
Algorithm"/>

```

0111	<AttributeValue type="Enumeration" value="AES"/>
0112	</Attribute>
0113	<Attribute>
0114	<AttributeName type="TextString" value="Cryptographic Length"/>
0115	<AttributeValue type="Integer" value="256"/>
0116	</Attribute>
0117	<Attribute>
0118	<AttributeName type="TextString" value="Digest"/>
0119	<AttributeValue>
0120	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0121	<DigestValue type="ByteString" value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046a1b931fdaed73591f29"/>
0122	<KeyFormatType type="Enumeration" value="Raw"/>
0123	</AttributeValue>
0124	</Attribute>
0125	<Attribute>
0126	<AttributeName type="TextString" value="Initial Date"/>
0127	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0128	</Attribute>
0129	<Attribute>
0130	<AttributeName type="TextString" value="Last Change Date"/>
0131	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0132	</Attribute>
0133	</ResponsePayload>
0134	</BatchItem>
0135	</ResponseMessage>
	<i># TIME 2</i>
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="Activate"/>
0146	<RequestPayload>
0147	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0148	</RequestPayload>
0149	</BatchItem>
0150	</RequestMessage>
0151	<ResponseMessage>
0152	<ResponseHeader>
0153	<ProtocolVersion>
0154	<ProtocolVersionMajor type="Integer" value="1"/>
0155	<ProtocolVersionMinor type="Integer" value="1"/>
0156	</ProtocolVersion>
0157	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0158	<BatchCount type="Integer" value="1"/>
0159	</ResponseHeader>
0160	<BatchItem>
0161	<Operation type="Enumeration" value="Activate"/>

0162	<ResultStatus type="Enumeration" value="Success"/>
0163	<ResponsePayload>
0164	<UniqueIdentifier type="TextString"
0165	value="\$UNIQUE_IDENTIFIER_0"/>
0166	</ResponsePayload>
0167	</BatchItem>
0168	</ResponseMessage>
0168	# TIME 3
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="GetAttributes"/>
0179	<RequestPayload>
0180	<UniqueIdentifier type="TextString"
0181	value="\$UNIQUE_IDENTIFIER_0"/>
0182	<AttributeName type="TextString" value="State"/>
0183	<AttributeName type="TextString" value="Activation Date"/>
0184	<AttributeName type="TextString" value="Deactivation Date"/>
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="2012-04-27T08:12:24+00:00"/>
0195	<BatchCount type="Integer" value="1"/>
0196	</ResponseHeader>
0197	<BatchItem>
0198	<Operation type="Enumeration" value="GetAttributes"/>
0199	<ResultStatus type="Enumeration" value="Success"/>
0200	<ResponsePayload>
0201	<UniqueIdentifier type="TextString"
0202	value="\$UNIQUE_IDENTIFIER_0"/>
0203	<Attribute>
0204	<AttributeName type="TextString" value="State"/>
0205	<AttributeValue type="Enumeration" value="Active"/>
0206	</Attribute>
0207	<Attribute>
0208	<AttributeName type="TextString" value="Activation Date"/>
0209	<AttributeValue type="DateTime" value="2013-01-
0210	10T23:36:01+00:00"/>
0211	</Attribute>
0212	</ResponsePayload>
0213	</BatchItem>
0214	</ResponseMessage>
0215	# TIME 4
0216	<RequestMessage>
0217	<RequestHeader>
0218	<ProtocolVersion>

0214	<ProtocolVersionMajor type="Integer" value="1"/>
0215	<ProtocolVersionMinor type="Integer" value="1"/>
0216	</ProtocolVersion>
0217	<BatchCount type="Integer" value="1"/>
0218	</RequestHeader>
0219	<BatchItem>
0220	<Operation type="Enumeration" value="Destroy"/>
0221	<RequestPayload>
0222	<UniqueIdentifier type="TextString" 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="Destroy"/>
0237	<ResultStatus type="Enumeration" value="OperationFailed"/>
0238	<ResultReason type="Enumeration" value="PermissionDenied"/>
0239	<ResultMessage type="TextString" value="DENIED"/>
0240	</BatchItem>
0241	</ResponseMessage>
0242	# TIME 5 <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="Revoke"/>
0252	<RequestPayload>
0253	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0254	<RevocationReason>
0255	<RevocationReasonCode type="Enumeration" value="KeyCompromise"/>
0256	</RevocationReason>
0257	<CompromiseOccurrenceDate type="DateTime" value="1970-01- 01T00:00:06+00:00"/>
0258	</RequestPayload>
0259	</BatchItem>
0260	</RequestMessage>
0261	<ResponseMessage>
0262	<ResponseHeader>
0263	<ProtocolVersion>
0264	<ProtocolVersionMajor type="Integer" value="1"/>
0265	<ProtocolVersionMinor type="Integer" value="1"/>
0266	</ProtocolVersion>

0267	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0268	<BatchCount type="Integer" value="1"/>
0269	</ResponseHeader>
0270	<BatchItem>
0271	<Operation type="Enumeration" value="Revoke"/>
0272	<ResultStatus type="Enumeration" value="Success"/>
0273	<ResponsePayload>
0274	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0275	</ResponsePayload>
0276	</BatchItem>
0277	</ResponseMessage>
	# TIME 6
0278	<RequestMessage>
0279	<RequestHeader>
0280	<ProtocolVersion>
0281	<ProtocolVersionMajor type="Integer" value="1"/>
0282	<ProtocolVersionMinor type="Integer" value="1"/>
0283	</ProtocolVersion>
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="State"/>
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="2012-04-27T08:12:24+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="State"/>
0310	<AttributeValue type="Enumeration" value="Compromised"/>
0311	</Attribute>
0312	</ResponsePayload>
0313	</BatchItem>
0314	</ResponseMessage>
	# TIME 7
0315	<RequestMessage>
0316	<RequestHeader>
0317	<ProtocolVersion>
0318	<ProtocolVersionMajor type="Integer" value="1"/>
0319	<ProtocolVersionMinor type="Integer" value="1"/>

0320	</ProtocolVersion>
0321	<BatchCount type="Integer" value="1"/>
0322	</RequestHeader>
0323	<BatchItem>
0324	<Operation type="Enumeration" value="Destroy"/>
0325	<RequestPayload>
0326	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0327	</RequestPayload>
0328	</BatchItem>
0329	</RequestMessage>
0330	<ResponseMessage>
0331	<ResponseHeader>
0332	<ProtocolVersion>
0333	<ProtocolVersionMajor type="Integer" value="1"/>
0334	<ProtocolVersionMinor type="Integer" value="1"/>
0335	</ProtocolVersion>
0336	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0337	<BatchCount type="Integer" value="1"/>
0338	</ResponseHeader>
0339	<BatchItem>
0340	<Operation type="Enumeration" value="Destroy"/>
0341	<ResultStatus type="Enumeration" value="Success"/>
0342	<ResponsePayload>
0343	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0344	</ResponsePayload>
0345	</BatchItem>
0346	</ResponseMessage>

118

119 3.2.3 SKLC-M-3-11

120 Create, GetAttributes, Activate, GetAttributes, Destroy, Revoke, GetAttributes, 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="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="Encrypt Decrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="SKLC-M-3-11"/>
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="2012-04-27T08:12:24+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="GetAttributes"/>
0065	<RequestPayload>
0066	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0067	<AttributeName type="TextString" value="State"/>
0068	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0069	<AttributeName type="TextString" value="Unique Identifier"/>
0070	<AttributeName type="TextString" value="Object Type"/>
0071	<AttributeName type="TextString" value="Cryptographic Algorithm"/>

```

0072     <AttributeName type="TextString" value="Cryptographic
Length"/>
0073     <AttributeName type="TextString" value="Digest"/>
0074     <AttributeName type="TextString" value="Initial Date"/>
0075     <AttributeName type="TextString" value="Last Change Date"/>
0076     </RequestPayload>
0077     </BatchItem>
0078 </RequestMessage>
0079 <ResponseMessage>
0080   <ResponseHeader>
0081     <ProtocolVersion>
0082       <ProtocolVersionMajor type="Integer" value="1"/>
0083       <ProtocolVersionMinor type="Integer" value="1"/>
0084     </ProtocolVersion>
0085     <TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0086     <BatchCount type="Integer" value="1"/>
0087   </ResponseHeader>
0088   <BatchItem>
0089     <Operation type="Enumeration" value="GetAttributes"/>
0090     <ResultStatus type="Enumeration" value="Success"/>
0091     <ResponsePayload>
0092       <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0093       <Attribute>
0094         <AttributeName type="TextString" value="State"/>
0095         <AttributeValue type="Enumeration" value="PreActive"/>
0096       </Attribute>
0097       <Attribute>
0098         <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0099         <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0100       </Attribute>
0101       <Attribute>
0102         <AttributeName type="TextString" value="Unique Identifier"/>
0103         <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0104       </Attribute>
0105       <Attribute>
0106         <AttributeName type="TextString" value="Object Type"/>
0107         <AttributeValue type="Enumeration" value="SymmetricKey"/>
0108       </Attribute>
0109       <Attribute>
0110         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0111         <AttributeValue type="Enumeration" value="AES"/>
0112       </Attribute>
0113       <Attribute>
0114         <AttributeName type="TextString" value="Cryptographic
Length"/>
0115         <AttributeValue type="Integer" value="256"/>
0116       </Attribute>
0117       <Attribute>
0118         <AttributeName type="TextString" value="Digest"/>
0119         <AttributeValue>
0120           <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0121           <DigestValue type="ByteString"
value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046a1b931fdaed73591
f29"/>

```

0122	<KeyFormatType type="Enumeration" value="Raw"/>
0123	</AttributeValue>
0124	</Attribute>
0125	<Attribute>
0126	<AttributeName type="TextString" value="Initial Date"/>
0127	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0128	</Attribute>
0129	</Attribute>
0130	<AttributeName type="TextString" value="Last Change Date"/>
0131	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0132	</Attribute>
0133	</ResponsePayload>
0134	</BatchItem>
0135	</ResponseMessage>
	<i># TIME 2</i>
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="Activate"/>
0146	<RequestPayload>
0147	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0148	</RequestPayload>
0149	</BatchItem>
0150	</RequestMessage>
0151	<ResponseMessage>
0152	<ResponseHeader>
0153	<ProtocolVersion>
0154	<ProtocolVersionMajor type="Integer" value="1"/>
0155	<ProtocolVersionMinor type="Integer" value="1"/>
0156	</ProtocolVersion>
0157	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0158	<BatchCount type="Integer" value="1"/>
0159	</ResponseHeader>
0160	<BatchItem>
0161	<Operation type="Enumeration" value="Activate"/>
0162	<ResultStatus type="Enumeration" value="Success"/>
0163	<ResponsePayload>
0164	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0165	</ResponsePayload>
0166	</BatchItem>
0167	</ResponseMessage>
	<i># TIME 3</i>
0168	<RequestMessage>
0169	<RequestHeader>
0170	<ProtocolVersion>
0171	<ProtocolVersionMajor type="Integer" value="1"/>
0172	<ProtocolVersionMinor type="Integer" value="1"/>
0173	</ProtocolVersion>

0174	<BatchCount type="Integer" value="1"/>
0175	</RequestHeader>
0176	<BatchItem>
0177	<Operation type="Enumeration" value="GetAttributes"/>
0178	<RequestPayload>
0179	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0180	<AttributeName type="TextString" value="State"/>
0181	<AttributeName type="TextString" value="Activation Date"/>
0182	<AttributeName type="TextString" value="Deactivation Date"/>
0183	</RequestPayload>
0184	</BatchItem>
0185	</RequestMessage>
0186	<ResponseMessage>
0187	<ResponseHeader>
0188	<ProtocolVersion>
0189	<ProtocolVersionMajor type="Integer" value="1"/>
0190	<ProtocolVersionMinor type="Integer" value="1"/>
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="GetAttributes"/>
0197	<ResultStatus type="Enumeration" value="Success"/>
0198	<ResponsePayload>
0199	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0200	<Attribute>
0201	<AttributeName type="TextString" value="State"/>
0202	<AttributeValue type="Enumeration" value="Active"/>
0203	</Attribute>
0204	<Attribute>
0205	<AttributeName type="TextString" value="Activation Date"/>
0206	<AttributeValue type="DateTime" value="2013-01- 10T23:36:01+00:00"/>
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	<BatchCount type="Integer" value="1"/>
0218	</RequestHeader>
0219	<BatchItem>
0220	<Operation type="Enumeration" value="ModifyAttribute"/>
0221	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0222	<RequestPayload>
0223	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0224	<Attribute>
0225	<AttributeName type="TextString" value="Activation Date"/>
0226	<AttributeValue type="DateTime" value="\$NOW"/>

0227	</Attribute>
0228	</RequestPayload>
0229	</BatchItem>
0230	</RequestMessage>
0231	<ResponseMessage>
0232	<ResponseHeader>
0233	<ProtocolVersion>
0234	<ProtocolVersionMajor type="Integer" value="1"/>
0235	<ProtocolVersionMinor type="Integer" value="1"/>
0236	</ProtocolVersion>
0237	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0238	<BatchCount type="Integer" value="1"/>
0239	</ResponseHeader>
0240	<BatchItem>
0241	<Operation type="Enumeration" value="ModifyAttribute"/>
0242	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0243	<ResultStatus type="Enumeration" value="OperationFailed"/>
0244	<ResultReason type="Enumeration" value="PermissionDenied"/>
0245	<ResultMessage type="TextString" value="DENIED"/>
0246	</BatchItem>
0247	</ResponseMessage>
	# TIME 5
0248	<RequestMessage>
0249	<RequestHeader>
0250	<ProtocolVersion>
0251	<ProtocolVersionMajor type="Integer" value="1"/>
0252	<ProtocolVersionMinor type="Integer" value="1"/>
0253	</ProtocolVersion>
0254	<BatchCount type="Integer" value="1"/>
0255	</RequestHeader>
0256	<BatchItem>
0257	<Operation type="Enumeration" value="Revoke"/>
0258	<RequestPayload>
0259	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0260	<RevocationReason>
0261	<RevocationReasonCode type="Enumeration" value="KeyCompromise"/>
0262	</RevocationReason>
0263	<CompromiseOccurrenceDate type="DateTime" value="1970-01-01T00:00:06+00:00"/>
0264	</RequestPayload>
0265	</BatchItem>
0266	</RequestMessage>
0267	<ResponseMessage>
0268	<ResponseHeader>
0269	<ProtocolVersion>
0270	<ProtocolVersionMajor type="Integer" value="1"/>
0271	<ProtocolVersionMinor type="Integer" value="1"/>
0272	</ProtocolVersion>
0273	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0274	<BatchCount type="Integer" value="1"/>
0275	</ResponseHeader>
0276	<BatchItem>
0277	<Operation type="Enumeration" value="Revoke"/>
0278	<ResultStatus type="Enumeration" value="Success"/>
0279	<ResponsePayload>
0280	<UniqueIdentifier type="TextString"

0281	value="\$UNIQUE_IDENTIFIER_0"/>
0282	</ResponsePayload>
0283	</BatchItem>
	</ResponseMessage>
	# TIME 6
0284	<RequestMessage>
0285	<RequestHeader>
0286	<ProtocolVersion>
0287	<ProtocolVersionMajor type="Integer" value="1"/>
0288	<ProtocolVersionMinor type="Integer" value="1"/>
0289	</ProtocolVersion>
0290	<BatchCount type="Integer" value="1"/>
0291	</RequestHeader>
0292	<BatchItem>
0293	<Operation type="Enumeration" value="GetAttributes"/>
0294	<RequestPayload>
0295	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0296	<AttributeName type="TextString" value="State"/>
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="2012-04-27T08:12:24+00:00"/>
0307	<BatchCount type="Integer" value="1"/>
0308	</ResponseHeader>
0309	<BatchItem>
0310	<Operation type="Enumeration" value="GetAttributes"/>
0311	<ResultStatus type="Enumeration" value="Success"/>
0312	<ResponsePayload>
0313	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0314	<Attribute>
0315	<AttributeName type="TextString" value="State"/>
0316	<AttributeValue type="Enumeration" value="Compromised"/>
0317	</Attribute>
0318	</ResponsePayload>
0319	</BatchItem>
0320	</ResponseMessage>
	# TIME 7
0321	<RequestMessage>
0322	<RequestHeader>
0323	<ProtocolVersion>
0324	<ProtocolVersionMajor type="Integer" value="1"/>
0325	<ProtocolVersionMinor type="Integer" value="1"/>
0326	</ProtocolVersion>
0327	<BatchCount type="Integer" value="1"/>
0328	</RequestHeader>
0329	<BatchItem>
0330	<Operation type="Enumeration" value="Destroy"/>
0331	<RequestPayload>
0332	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0333	</RequestPayload>
0334	</BatchItem>
0335	</RequestMessage>
0336	<ResponseMessage>
0337	<ResponseHeader>
0338	<ProtocolVersion>
0339	<ProtocolVersionMajor type="Integer" value="1"/>
0340	<ProtocolVersionMinor type="Integer" value="1"/>
0341	</ProtocolVersion>
0342	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0343	<BatchCount type="Integer" value="1"/>
0344	</ResponseHeader>
0345	<BatchItem>
0346	<Operation type="Enumeration" value="Destroy"/>
0347	<ResultStatus type="Enumeration" value="Success"/>
0348	<ResponsePayload>
0349	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0350	</ResponsePayload>
0351	</BatchItem>
0352	</ResponseMessage>

121

122 3.3 Mandatory Test Cases KMIP v1.2

123 3.3.1 SKLC-M-1-12

124 Create, GetAttributes, 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="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="Encrypt Decrypt"/>
0025	</Attribute>

0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="SKLC-M-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="2012-04-27T08:12:24+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="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	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0069	<AttributeName type="TextString" value="Unique Identifier"/>
0070	<AttributeName type="TextString" value="Object Type"/>
0071	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0072	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0073	<AttributeName type="TextString" value="Digest"/>
0074	<AttributeName type="TextString" value="Initial Date"/>
0075	<AttributeName type="TextString" value="Last Change Date"/>
0076	<AttributeName type="TextString" value="Activation Date"/>

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="2012-04-27T08:12:24+00:00"/>
0087	<BatchCount type="Integer" value="1"/>
0088	</ResponseHeader>
0089	<BatchItem>
0090	<Operation type="Enumeration" value="GetAttributes"/>
0091	<ResultStatus type="Enumeration" value="Success"/>
0092	<ResponsePayload>
0093	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0094	<Attribute>
0095	<AttributeName type="TextString" value="State"/>
0096	<AttributeValue type="Enumeration" value="PreActive"/>
0097	</Attribute>
0098	<Attribute>
0099	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0100	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0101	</Attribute>
0102	<Attribute>
0103	<AttributeName type="TextString" value="Unique Identifier"/>
0104	<AttributeValue type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0105	</Attribute>
0106	<Attribute>
0107	<AttributeName type="TextString" value="Object Type"/>
0108	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0109	</Attribute>
0110	<Attribute>
0111	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0112	<AttributeValue type="Enumeration" value="AES"/>
0113	</Attribute>
0114	<Attribute>
0115	<AttributeName type="TextString" value="Cryptographic Length"/>
0116	<AttributeValue type="Integer" value="256"/>
0117	</Attribute>
0118	<Attribute>
0119	<AttributeName type="TextString" value="Digest"/>
0120	<AttributeValue>
0121	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0122	<DigestValue type="ByteString" value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046a1b931fdaed73591 f29"/>
0123	<KeyFormatType type="Enumeration" value="Raw"/>
0124	</AttributeValue>
0125	</Attribute>
0126	<Attribute>
0127	<AttributeName type="TextString" value="Initial Date"/>

0128	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0129	</Attribute>
0130	<Attribute>
0131	<AttributeName type="TextString" value="Last Change Date"/>
0132	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0133	</Attribute>
0134	</ResponsePayload>
0135	</BatchItem>
0136	</ResponseMessage>
0137	# TIME 2 <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="Destroy"/>
0147	<RequestPayload>
0148	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0149	</RequestPayload>
0150	</BatchItem>
0151	</RequestMessage>
0152	<ResponseMessage>
0153	<ResponseHeader>
0154	<ProtocolVersion>
0155	<ProtocolVersionMajor type="Integer" value="1"/>
0156	<ProtocolVersionMinor type="Integer" value="2"/>
0157	</ProtocolVersion>
0158	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0159	<BatchCount type="Integer" value="1"/>
0160	</ResponseHeader>
0161	<BatchItem>
0162	<Operation type="Enumeration" value="Destroy"/>
0163	<ResultStatus type="Enumeration" value="Success"/>
0164	<ResponsePayload>
0165	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0166	</ResponsePayload>
0167	</BatchItem>
0168	</ResponseMessage>

125

126 3.3.2 SKLC-M-2-12

127 Create, GetAttributes, Activate, GetAttributes, Destroy, Revoke, GetAttributes, 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="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="Encrypt Decrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="SKLC-M-2-12"/>
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="2012-04-27T08:12:24+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="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="$UNIQUE_IDENTIFIER_0"/>
0067             <AttributeName type="TextString" value="State"/>
0068             <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0069             <AttributeName type="TextString" value="Unique Identifier"/>
0070             <AttributeName type="TextString" value="Object Type"/>
0071             <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0072             <AttributeName type="TextString" value="Cryptographic
Length"/>
0073             <AttributeName type="TextString" value="Digest"/>
0074             <AttributeName type="TextString" value="Initial Date"/>
0075             <AttributeName type="TextString" value="Last Change Date"/>
0076         </RequestPayload>
0077     </BatchItem>
0078 </RequestMessage>
0079 <ResponseMessage>
0080     <ResponseHeader>
0081         <ProtocolVersion>
0082             <ProtocolVersionMajor type="Integer" value="1"/>
0083             <ProtocolVersionMinor type="Integer" value="2"/>
0084         </ProtocolVersion>
0085         <TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0086         <BatchCount type="Integer" value="1"/>
0087     </ResponseHeader>
0088     <BatchItem>
0089         <Operation type="Enumeration" value="GetAttributes"/>
0090         <ResultStatus type="Enumeration" value="Success"/>
0091         <ResponsePayload>
0092             <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0093             <Attribute>
0094                 <AttributeName type="TextString" value="State"/>
0095                 <AttributeValue type="Enumeration" value="PreActive"/>
0096             </Attribute>
0097             <Attribute>
0098                 <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0099                 <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0100             </Attribute>
0101             <Attribute>
0102                 <AttributeName type="TextString" value="Unique Identifier"/>
0103                 <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0104             </Attribute>
0105             <Attribute>
0106                 <AttributeName type="TextString" value="Object Type"/>
0107                 <AttributeValue type="Enumeration" value="SymmetricKey"/>
0108             </Attribute>

```

0109	<Attribute>
0110	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0111	<AttributeValue type="Enumeration" value="AES"/>
0112	</Attribute>
0113	<Attribute>
0114	<AttributeName type="TextString" value="Cryptographic Length"/>
0115	<AttributeValue type="Integer" value="256"/>
0116	</Attribute>
0117	<Attribute>
0118	<AttributeName type="TextString" value="Digest"/>
0119	<AttributeValue>
0120	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0121	<DigestValue type="ByteString" value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046a1b931fdaed73591f29"/>
0122	<KeyFormatType type="Enumeration" value="Raw"/>
0123	</AttributeValue>
0124	</Attribute>
0125	<Attribute>
0126	<AttributeName type="TextString" value="Initial Date"/>
0127	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0128	</Attribute>
0129	<Attribute>
0130	<AttributeName type="TextString" value="Last Change Date"/>
0131	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0132	</Attribute>
0133	</ResponsePayload>
0134	</BatchItem>
0135	</ResponseMessage>
	# TIME 2
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="Activate"/>
0146	<RequestPayload>
0147	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0148	</RequestPayload>
0149	</BatchItem>
0150	</RequestMessage>
0151	<ResponseMessage>
0152	<ResponseHeader>
0153	<ProtocolVersion>
0154	<ProtocolVersionMajor type="Integer" value="1"/>
0155	<ProtocolVersionMinor type="Integer" value="2"/>
0156	</ProtocolVersion>
0157	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0158	<BatchCount type="Integer" value="1"/>

0159	</ResponseHeader>
0160	<BatchItem>
0161	<Operation type="Enumeration" value="Activate"/>
0162	<ResultStatus type="Enumeration" value="Success"/>
0163	<ResponsePayload>
0164	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0165	</ResponsePayload>
0166	</BatchItem>
0167	</ResponseMessage>
# TIME 3	
0168	<RequestMessage>
0169	<RequestHeader>
0170	<ProtocolVersion>
0171	<ProtocolVersionMajor type="Integer" value="1"/>
0172	<ProtocolVersionMinor type="Integer" value="2"/>
0173	</ProtocolVersion>
0174	<BatchCount type="Integer" value="1"/>
0175	</RequestHeader>
0176	<BatchItem>
0177	<Operation type="Enumeration" value="GetAttributes"/>
0178	<RequestPayload>
0179	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0180	<AttributeName type="TextString" value="State"/>
0181	<AttributeName type="TextString" value="Activation Date"/>
0182	<AttributeName type="TextString" value="Deactivation Date"/>
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="GetAttributes"/>
0197	<ResultStatus type="Enumeration" value="Success"/>
0198	<ResponsePayload>
0199	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0200	<Attribute>
0201	<AttributeName type="TextString" value="State"/>
0202	<AttributeValue type="Enumeration" value="Active"/>
0203	</Attribute>
0204	<Attribute>
0205	<AttributeName type="TextString" value="Activation Date"/>
0206	<AttributeValue type="DateTime" value="2013-01- 10T23:36:01+00:00"/>
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	<BatchCount type="Integer" value="1"/>
0218	</RequestHeader>
0219	<BatchItem>
0220	<Operation type="Enumeration" value="Destroy"/>
0221	<RequestPayload>
0222	<UniqueIdentifier type="TextString"
	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="2"/>
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="Destroy"/>
0237	<ResultStatus type="Enumeration" value="OperationFailed"/>
0238	<ResultReason type="Enumeration" value="PermissionDenied"/>
0239	<ResultMessage type="TextString" value="DENIED"/>
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="Revoke"/>
0252	<RequestPayload>
0253	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0254	<RevocationReason>
0255	<RevocationReasonCode type="Enumeration"
	value="KeyCompromise"/>
0256	</RevocationReason>
0257	<CompromiseOccurrenceDate type="DateTime" value="1970-01-
	01T00:00:06+00:00"/>
0258	</RequestPayload>
0259	</BatchItem>
0260	</RequestMessage>
0261	<ResponseMessage>
0262	<ResponseHeader>
0263	<ProtocolVersion>

0264	<ProtocolVersionMajor type="Integer" value="1"/>
0265	<ProtocolVersionMinor type="Integer" value="2"/>
0266	</ProtocolVersion>
0267	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0268	<BatchCount type="Integer" value="1"/>
0269	</ResponseHeader>
0270	<BatchItem>
0271	<Operation type="Enumeration" value="Revoke"/>
0272	<ResultStatus type="Enumeration" value="Success"/>
0273	<ResponsePayload>
0274	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0275	</ResponsePayload>
0276	</BatchItem>
0277	</ResponseMessage>
	# TIME 6
0278	<RequestMessage>
0279	<RequestHeader>
0280	<ProtocolVersion>
0281	<ProtocolVersionMajor type="Integer" value="1"/>
0282	<ProtocolVersionMinor type="Integer" value="2"/>
0283	</ProtocolVersion>
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="State"/>
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="2012-04-27T08:12:24+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="State"/>
0310	<AttributeValue type="Enumeration" value="Compromised"/>
0311	</Attribute>
0312	</ResponsePayload>
0313	</BatchItem>
0314	</ResponseMessage>
	# TIME 7
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="Destroy"/>
0325	<RequestPayload>
0326	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0327	</RequestPayload>
0328	</BatchItem>
0329	</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="2012-04-27T08:12:25+00:00"/>
0337	<BatchCount type="Integer" value="1"/>
0338	</ResponseHeader>
0339	<BatchItem>
0340	<Operation type="Enumeration" value="Destroy"/>
0341	<ResultStatus type="Enumeration" value="Success"/>
0342	<ResponsePayload>
0343	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0344	</ResponsePayload>
0345	</BatchItem>
0346	</ResponseMessage>

128

129 3.3.3 SKLC-M-3-12

130 Create, GetAttributes, Activate, GetAttributes, Destroy, Revoke, GetAttributes, 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="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="Encrypt Decrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="SKLC-M-3-12"/>
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="2012-04-27T08:12:24+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="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	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0069	<AttributeName type="TextString" value="Unique Identifier"/>

0070	<AttributeName type="TextString" value="Object Type"/>
0071	<AttributeName type="TextString" value="Cryptographic
0072	Algorithm"/> <AttributeName type="TextString" value="Cryptographic
0073	Length"/>
0074	<AttributeName type="TextString" value="Digest"/>
0075	<AttributeName type="TextString" value="Initial Date"/>
0076	<AttributeName type="TextString" value="Last Change Date"/>
0077	</RequestPayload>
0078	</BatchItem> </RequestMessage>
0079	<ResponseMessage>
0080	<ResponseHeader>
0081	<ProtocolVersion>
0082	<ProtocolVersionMajor type="Integer" value="1"/>
0083	<ProtocolVersionMinor type="Integer" value="2"/>
0084	</ProtocolVersion>
0085	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0086	<BatchCount type="Integer" value="1"/>
0087	</ResponseHeader>
0088	<BatchItem>
0089	<Operation type="Enumeration" value="GetAttributes"/>
0090	<ResultStatus type="Enumeration" value="Success"/>
0091	<ResponsePayload>
0092	<UniqueIdentifier type="TextString"
0093	value="\$UNIQUE_IDENTIFIER_0"/>
0094	<Attribute>
0095	<AttributeName type="TextString" value="State"/>
0096	<AttributeValue type="Enumeration" value="PreActive"/>
0097	</Attribute>
0098	<Attribute>
0099	<AttributeName type="TextString" value="Cryptographic Usage
0100	Mask"/>
0101	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0102	</Attribute>
0103	<Attribute>
0104	<AttributeName type="TextString" value="Unique Identifier"/>
0105	<AttributeValue type="TextString"
0106	value="\$UNIQUE_IDENTIFIER_0"/>
0107	</Attribute>
0108	<Attribute>
0109	<AttributeName type="TextString" value="Object Type"/>
0110	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0111	</Attribute>
0112	<Attribute>
0113	<AttributeName type="TextString" value="Cryptographic
0114	Length"/>
0115	<AttributeValue type="Integer" value="256"/>
0116	</Attribute>
0117	<Attribute>
0118	<AttributeName type="TextString" value="Digest"/>
0119	<AttributeValue>
0120	<HashingAlgorithm type="Enumeration" value="SHA 256"/>

0121	<DigestValue type="ByteString" value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046a1b931fdaed73591 f29"/>
0122	<KeyFormatType type="Enumeration" value="Raw"/>
0123	</AttributeValue>
0124	</Attribute>
0125	<Attribute>
0126	<AttributeName type="TextString" value="Initial Date"/>
0127	<AttributeValue type="DateTime" value="2013-01- 10T23:33:21+00:00"/>
0128	</Attribute>
0129	<Attribute>
0130	<AttributeName type="TextString" value="Last Change Date"/>
0131	<AttributeValue type="DateTime" value="2013-01- 10T23:33:21+00:00"/>
0132	</Attribute>
0133	</ResponsePayload>
0134	</BatchItem>
0135	</ResponseMessage>
	# TIME 2
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="Activate"/>
0146	<RequestPayload>
0147	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0148	</RequestPayload>
0149	</BatchItem>
0150	</RequestMessage>
0151	<ResponseMessage>
0152	<ResponseHeader>
0153	<ProtocolVersion>
0154	<ProtocolVersionMajor type="Integer" value="1"/>
0155	<ProtocolVersionMinor type="Integer" value="2"/>
0156	</ProtocolVersion>
0157	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0158	<BatchCount type="Integer" value="1"/>
0159	</ResponseHeader>
0160	<BatchItem>
0161	<Operation type="Enumeration" value="Activate"/>
0162	<ResultStatus type="Enumeration" value="Success"/>
0163	<ResponsePayload>
0164	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0165	</ResponsePayload>
0166	</BatchItem>
0167	</ResponseMessage>
	# TIME 3
0168	<RequestMessage>
0169	<RequestHeader>
0170	<ProtocolVersion>

0171	<ProtocolVersionMajor type="Integer" value="1"/>
0172	<ProtocolVersionMinor type="Integer" value="2"/>
0173	</ProtocolVersion>
0174	<BatchCount type="Integer" value="1"/>
0175	</RequestHeader>
0176	<BatchItem>
0177	<Operation type="Enumeration" value="GetAttributes"/>
0178	<RequestPayload>
0179	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0180	<AttributeName type="TextString" value="State"/>
0181	<AttributeName type="TextString" value="Activation Date"/>
0182	<AttributeName type="TextString" value="Deactivation Date"/>
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="GetAttributes"/>
0197	<ResultStatus type="Enumeration" value="Success"/>
0198	<ResponsePayload>
0199	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0200	<Attribute>
0201	<AttributeName type="TextString" value="State"/>
0202	<AttributeValue type="Enumeration" value="Active"/>
0203	</Attribute>
0204	<Attribute>
0205	<AttributeName type="TextString" value="Activation Date"/>
0206	<AttributeValue type="DateTime" value="2013-01-
	10T23:36:01+00:00"/>
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	<BatchCount type="Integer" value="1"/>
0218	</RequestHeader>
0219	<BatchItem>
0220	<Operation type="Enumeration" value="ModifyAttribute"/>
0221	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0222	<RequestPayload>
0223	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>

0224	<Attribute>
0225	<AttributeName type="TextString" value="Activation Date"/>
0226	<AttributeValue type="DateTime" value="\$NOW"/>
0227	</Attribute>
0228	</RequestPayload>
0229	</BatchItem>
0230	</RequestMessage>
0231	<ResponseMessage>
0232	<ResponseHeader>
0233	<ProtocolVersion>
0234	<ProtocolVersionMajor type="Integer" value="1"/>
0235	<ProtocolVersionMinor type="Integer" value="2"/>
0236	</ProtocolVersion>
0237	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0238	<BatchCount type="Integer" value="1"/>
0239	</ResponseHeader>
0240	<BatchItem>
0241	<Operation type="Enumeration" value="ModifyAttribute"/>
0242	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0243	<ResultStatus type="Enumeration" value="OperationFailed"/>
0244	<ResultReason type="Enumeration" value="PermissionDenied"/>
0245	<ResultMessage type="TextString" value="DENIED"/>
0246	</BatchItem>
0247	</ResponseMessage>
0248	# TIME 5 <RequestMessage>
0249	<RequestHeader>
0250	<ProtocolVersion>
0251	<ProtocolVersionMajor type="Integer" value="1"/>
0252	<ProtocolVersionMinor type="Integer" value="2"/>
0253	</ProtocolVersion>
0254	<BatchCount type="Integer" value="1"/>
0255	</RequestHeader>
0256	<BatchItem>
0257	<Operation type="Enumeration" value="Revoke"/>
0258	<RequestPayload>
0259	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0260	<RevocationReason>
0261	<RevocationReasonCode type="Enumeration" value="KeyCompromise"/>
0262	</RevocationReason>
0263	<CompromiseOccurrenceDate type="DateTime" value="1970-01- 01T00:00:06+00:00"/>
0264	</RequestPayload>
0265	</BatchItem>
0266	</RequestMessage>
0267	<ResponseMessage>
0268	<ResponseHeader>
0269	<ProtocolVersion>
0270	<ProtocolVersionMajor type="Integer" value="1"/>
0271	<ProtocolVersionMinor type="Integer" value="2"/>
0272	</ProtocolVersion>
0273	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0274	<BatchCount type="Integer" value="1"/>
0275	</ResponseHeader>
0276	<BatchItem>
0277	<Operation type="Enumeration" value="Revoke"/>

0278	<ResultStatus type="Enumeration" value="Success"/>
0279	<ResponsePayload>
0280	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0281	</ResponsePayload>
0282	</BatchItem>
0283	</ResponseMessage>
	# TIME 6
0284	<RequestMessage>
0285	<RequestHeader>
0286	<ProtocolVersion>
0287	<ProtocolVersionMajor type="Integer" value="1"/>
0288	<ProtocolVersionMinor type="Integer" value="2"/>
0289	</ProtocolVersion>
0290	<BatchCount type="Integer" value="1"/>
0291	</RequestHeader>
0292	<BatchItem>
0293	<Operation type="Enumeration" value="GetAttributes"/>
0294	<RequestPayload>
0295	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0296	<AttributeName type="TextString" value="State"/>
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="2012-04-27T08:12:24+00:00"/>
0307	<BatchCount type="Integer" value="1"/>
0308	</ResponseHeader>
0309	<BatchItem>
0310	<Operation type="Enumeration" value="GetAttributes"/>
0311	<ResultStatus type="Enumeration" value="Success"/>
0312	<ResponsePayload>
0313	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0314	<Attribute>
0315	<AttributeName type="TextString" value="State"/>
0316	<AttributeValue type="Enumeration" value="Compromised"/>
0317	</Attribute>
0318	</ResponsePayload>
0319	</BatchItem>
0320	</ResponseMessage>
	# TIME 7
0321	<RequestMessage>
0322	<RequestHeader>
0323	<ProtocolVersion>
0324	<ProtocolVersionMajor type="Integer" value="1"/>
0325	<ProtocolVersionMinor type="Integer" value="2"/>
0326	</ProtocolVersion>
0327	<BatchCount type="Integer" value="1"/>
0328	</RequestHeader>
0329	<BatchItem>
0330	<Operation type="Enumeration" value="Destroy"/>

0331	<RequestPayload>
0332	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0333	</RequestPayload>
0334	</BatchItem>
0335	</RequestMessage>
0336	<ResponseMessage>
0337	<ResponseHeader>
0338	<ProtocolVersion>
0339	<ProtocolVersionMajor type="Integer" value="1"/>
0340	<ProtocolVersionMinor type="Integer" value="2"/>
0341	</ProtocolVersion>
0342	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0343	<BatchCount type="Integer" value="1"/>
0344	</ResponseHeader>
0345	<BatchItem>
0346	<Operation type="Enumeration" value="Destroy"/>
0347	<ResultStatus type="Enumeration" value="Success"/>
0348	<ResponsePayload>
0349	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0350	</ResponsePayload>
0351	</BatchItem>
0352	</ResponseMessage>

131

132 3.4 Optional Test Cases KMIP v1.0

133 3.4.1 SKLC-O-1-10

134 Create, GetAttributes, Destroy, GetAttributes

	<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 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="Encrypt Decrypt"/>
0026	</Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="SKLC-O-1-10"/>
0030	<NameType type="Enumeration"
0031	value="UninterpretedTextString"/>
0032	</AttributeValue>
0033	</Attribute>
0034	</TemplateAttribute>
0035	</RequestPayload>
0036	</BatchItem>
0037	</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="2012-04-27T08:12:24+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>
0055	# TIME 1
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="GetAttributes"/>
0066	<RequestPayload>
0067	<UniqueIdentifier type="TextString"
0068	value="\$UNIQUE_IDENTIFIER_0"/>
0069	<AttributeName type="TextString" value="State"/>
0070	<AttributeName type="TextString" value="Cryptographic Usage
0071	Mask"/>
0072	<AttributeName type="TextString" value="Unique Identifier"/>
0073	<AttributeName type="TextString" value="Object Type"/>
0074	<AttributeName type="TextString" value="Cryptographic
0075	Algorithm"/>
0076	<AttributeName type="TextString" value="Cryptographic
0077	Length"/>
0078	<AttributeName type="TextString" value="Digest"/>

0074	<AttributeName type="TextString" value="Initial Date"/>
0075	<AttributeName type="TextString" value="Last Change Date"/>
0076	<AttributeName type="TextString" value="Activation Date"/>
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="2012-04-27T08:12:24+00:00"/>
0087	<BatchCount type="Integer" value="1"/>
0088	</ResponseHeader>
0089	<BatchItem>
0090	<Operation type="Enumeration" value="GetAttributes"/>
0091	<ResultStatus type="Enumeration" value="Success"/>
0092	<ResponsePayload>
0093	<UniqueIdentifier type="TextString"
0094	value="\$UNIQUE_IDENTIFIER_0"/>
0095	<Attribute>
0096	<AttributeName type="TextString" value="State"/>
0097	<AttributeValue type="Enumeration" value="PreActive"/>
0098	</Attribute>
0099	<AttributeName type="TextString" value="Cryptographic Usage
0100	Mask"/>
0101	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0102	</Attribute>
0103	<AttributeName type="TextString" value="Unique Identifier"/>
0104	<AttributeValue type="TextString"
0105	value="\$UNIQUE_IDENTIFIER_0"/>
0106	</Attribute>
0107	<AttributeName type="TextString" value="Object Type"/>
0108	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0109	</Attribute>
0110	<Attribute>
0111	<AttributeName type="TextString" value="Cryptographic
0112	Algorithm"/>
0113	<AttributeValue type="Enumeration" value="AES"/>
0114	</Attribute>
0115	<AttributeName type="TextString" value="Cryptographic
0116	Length"/>
0117	<AttributeValue type="Integer" value="256"/>
0118	</Attribute>
0119	<AttributeName type="TextString" value="Digest"/>
0120	<AttributeValue>
0121	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0122	<DigestValue type="ByteString"
0123	value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046a1b931fdaed73591
0124	f29"/>

0125	<Attribute>
0126	<AttributeName type="TextString" value="Initial Date"/>
0127	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0128	</Attribute>
0129	<Attribute>
0130	<AttributeName type="TextString" value="Last Change Date"/>
0131	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0132	</Attribute>
0133	</ResponsePayload>
0134	</BatchItem>
0135	</ResponseMessage>
# TIME 2	
0136	<RequestMessage>
0137	<RequestHeader>
0138	<ProtocolVersion>
0139	<ProtocolVersionMajor type="Integer" value="1"/>
0140	<ProtocolVersionMinor type="Integer" value="0"/>
0141	</ProtocolVersion>
0142	<BatchCount type="Integer" value="1"/>
0143	</RequestHeader>
0144	<BatchItem>
0145	<Operation type="Enumeration" value="Destroy"/>
0146	<RequestPayload>
0147	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0148	</RequestPayload>
0149	</BatchItem>
0150	</RequestMessage>
# TIME 3	
0151	<ResponseMessage>
0152	<ResponseHeader>
0153	<ProtocolVersion>
0154	<ProtocolVersionMajor type="Integer" value="1"/>
0155	<ProtocolVersionMinor type="Integer" value="0"/>
0156	</ProtocolVersion>
0157	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0158	<BatchCount type="Integer" value="1"/>
0159	</ResponseHeader>
0160	<BatchItem>
0161	<Operation type="Enumeration" value="Destroy"/>
0162	<ResultStatus type="Enumeration" value="Success"/>
0163	<ResponsePayload>
0164	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0165	</ResponsePayload>
0166	</BatchItem>
0167	</ResponseMessage>
# TIME 3	
0168	<RequestMessage>
0169	<RequestHeader>
0170	<ProtocolVersion>
0171	<ProtocolVersionMajor type="Integer" value="1"/>
0172	<ProtocolVersionMinor type="Integer" value="0"/>
0173	</ProtocolVersion>
0174	<BatchCount type="Integer" value="1"/>
0175	</RequestHeader>
0176	<BatchItem>

0177	<Operation type="Enumeration" value="GetAttributes"/>
0178	<RequestPayload>
0179	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
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="2012-04-27T08:12:25+00:00"/>
0190	<BatchCount type="Integer" value="1"/>
0191	</ResponseHeader>
0192	<BatchItem>
0193	<Operation type="Enumeration" value="GetAttributes"/>
0194	<ResultStatus type="Enumeration" value="Success"/>
0195	<ResponsePayload>
0196	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0197	<Attribute>
0198	<AttributeName type="TextString" value="Unique Identifier"/>
0199	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0200	</Attribute>
0201	<Attribute>
0202	<AttributeName type="TextString" value="Object Type"/>
0203	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0204	</Attribute>
0205	<Attribute>
0206	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0207	<AttributeValue type="Enumeration" value="AES"/>
0208	</Attribute>
0209	<Attribute>
0210	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0211	<AttributeValue type="Integer" value="256"/>
0212	</Attribute>
0213	<Attribute>
0214	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0215	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0216	</Attribute>
0217	<Attribute>
0218	<AttributeName type="TextString" value="Destroy Date"/>
0219	<AttributeValue type="DateTime" value="2013-01-
	11T00:39:11+00:00"/>
0220	</Attribute>
0221	<Attribute>
0222	<AttributeName type="TextString" value="Digest"/>
0223	<AttributeValue>
0224	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0225	<DigestValue type="ByteString"
	value="bf60cac2a3f82e6added839c87b0bdbbc386d6280c14c8f09ca96e098365f7
	fe3"/>

```

0226     </AttributeValue>
0227     </Attribute>
0228     <Attribute>
0229         <AttributeName type="TextString" value="Initial Date"/>
0230         <AttributeValue type="DateTime" value="2013-01-
11T00:39:11+00:00"/>
0231     </Attribute>
0232     <Attribute>
0233         <AttributeName type="TextString" value="Last Change Date"/>
0234         <AttributeValue type="DateTime" value="2013-01-
11T00:39:11+00:00"/>
0235     </Attribute>
0236     <Attribute>
0237         <AttributeName type="TextString" value="Lease Time"/>
0238         <AttributeValue type="Interval" value="3600"/>
0239     </Attribute>
0240     <Attribute>
0241         <AttributeName type="TextString" value="Name"/>
0242         <AttributeValue>
0243             <NameValue type="TextString" value="SKLC-O-1-10"/>
0244             <NameType type="Enumeration"
value="UninterpretedTextString"/>
0245         </AttributeValue>
0246     </Attribute>
0247     <Attribute>
0248         <AttributeName type="TextString" value="State"/>
0249         <AttributeValue type="Enumeration" value="Destroyed"/>
0250     </Attribute>
0251 </ResponsePayload>
0252 </BatchItem>
0253 </ResponseMessage>

```

135

136 3.5 Optional Test Cases KMIP v1.1

137 3.5.1 SKLC-O-1-11

138 Create, GetAttributes, Destroy, GetAttributes

```

0001 # 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="Encrypt Decrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="SKLC-O-1-11"/>
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="2012-04-27T08:12:24+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="GetAttributes"/>
0065	<RequestPayload>
0066	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0067	<AttributeName type="TextString" value="State"/>
0068	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>

```

0069     <AttributeName type="TextString" value="Unique Identifier"/>
0070     <AttributeName type="TextString" value="Object Type"/>
0071     <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0072     <AttributeName type="TextString" value="Cryptographic
Length"/>
0073     <AttributeName type="TextString" value="Digest"/>
0074     <AttributeName type="TextString" value="Initial Date"/>
0075     <AttributeName type="TextString" value="Last Change Date"/>
0076     <AttributeName type="TextString" value="Activation Date"/>
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="2012-04-27T08:12:24+00:00"/>
0087     <BatchCount type="Integer" value="1"/>
0088   </ResponseHeader>
0089   <BatchItem>
0090     <Operation type="Enumeration" value="GetAttributes"/>
0091     <ResultStatus type="Enumeration" value="Success"/>
0092     <ResponsePayload>
0093       <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0094       <Attribute>
0095         <AttributeName type="TextString" value="State"/>
0096         <AttributeValue type="Enumeration" value="PreActive"/>
0097       </Attribute>
0098       <Attribute>
0099         <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0100         <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0101       </Attribute>
0102       <Attribute>
0103         <AttributeName type="TextString" value="Unique Identifier"/>
0104         <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0105       </Attribute>
0106       <Attribute>
0107         <AttributeName type="TextString" value="Object Type"/>
0108         <AttributeValue type="Enumeration" value="SymmetricKey"/>
0109       </Attribute>
0110       <Attribute>
0111         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0112         <AttributeValue type="Enumeration" value="AES"/>
0113       </Attribute>
0114       <Attribute>
0115         <AttributeName type="TextString" value="Cryptographic
Length"/>
0116         <AttributeValue type="Integer" value="256"/>
0117       </Attribute>
0118       <Attribute>
0119         <AttributeName type="TextString" value="Digest"/>

```

0120	<AttributeValue>
0121	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0122	<DigestValue type="ByteString" value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046a1b931fdaed73591f29"/>
0123	<KeyFormatType type="Enumeration" value="Raw"/>
0124	</AttributeValue>
0125	</Attribute>
0126	<Attribute>
0127	<AttributeName type="TextString" value="Initial Date"/>
0128	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0129	</Attribute>
0130	<Attribute>
0131	<AttributeName type="TextString" value="Last Change Date"/>
0132	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0133	</Attribute>
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="Destroy"/>
0147	<RequestPayload>
0148	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0149	</RequestPayload>
0150	</BatchItem>
0151	</RequestMessage>
0152	<ResponseMessage>
0153	<ResponseHeader>
0154	<ProtocolVersion>
0155	<ProtocolVersionMajor type="Integer" value="1"/>
0156	<ProtocolVersionMinor type="Integer" value="1"/>
0157	</ProtocolVersion>
0158	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0159	<BatchCount type="Integer" value="1"/>
0160	</ResponseHeader>
0161	<BatchItem>
0162	<Operation type="Enumeration" value="Destroy"/>
0163	<ResultStatus type="Enumeration" value="Success"/>
0164	<ResponsePayload>
0165	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
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="1"/>
0174   </ProtocolVersion>
0175   <BatchCount type="Integer" value="1"/>
0176 </RequestHeader>
0177 <BatchItem>
0178   <Operation type="Enumeration" value="GetAttributes"/>
0179   <RequestPayload>
0180     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0181   </RequestPayload>
0182 </BatchItem>
0183 </RequestMessage>
0184 <ResponseMessage>
0185   <ResponseHeader>
0186     <ProtocolVersion>
0187       <ProtocolVersionMajor type="Integer" value="1"/>
0188       <ProtocolVersionMinor type="Integer" value="1"/>
0189     </ProtocolVersion>
0190     <TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0191     <BatchCount type="Integer" value="1"/>
0192   </ResponseHeader>
0193   <BatchItem>
0194     <Operation type="Enumeration" value="GetAttributes"/>
0195     <ResultStatus type="Enumeration" value="Success"/>
0196     <ResponsePayload>
0197       <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0198       <Attribute>
0199         <AttributeName type="TextString" value="Unique Identifier"/>
0200         <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0201       </Attribute>
0202       <Attribute>
0203         <AttributeName type="TextString" value="Object Type"/>
0204         <AttributeValue type="Enumeration" value="SymmetricKey"/>
0205       </Attribute>
0206       <Attribute>
0207         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0208         <AttributeValue type="Enumeration" value="AES"/>
0209       </Attribute>
0210       <Attribute>
0211         <AttributeName type="TextString" value="Cryptographic
Length"/>
0212         <AttributeValue type="Integer" value="256"/>
0213       </Attribute>
0214       <Attribute>
0215         <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0216         <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0217       </Attribute>
0218       <Attribute>
0219         <AttributeName type="TextString" value="Destroy Date"/>
0220         <AttributeValue type="DateTime" value="2013-01-
11T00:39:11+00:00"/>

```

```

0221     </Attribute>
0222     <Attribute>
0223         <AttributeName type="TextString" value="Digest"/>
0224         <AttributeValue>
0225             <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0226             <DigestValue type="ByteString"
value="bf60cac2a3f82e6added839c87b0bdbcb386d6280c14c8f09ca96e098365f7
fe3"/>
0227             <KeyFormatType type="Enumeration" value="Raw"/>
0228         </AttributeValue>
0229     </Attribute>
0230     <Attribute>
0231         <AttributeName type="TextString" value="Fresh"/>
0232         <AttributeValue type="Boolean" value="true"/>
0233     </Attribute>
0234     <Attribute>
0235         <AttributeName type="TextString" value="Initial Date"/>
0236         <AttributeValue type="DateTime" value="2013-01-
11T00:39:11+00:00"/>
0237     </Attribute>
0238     <Attribute>
0239         <AttributeName type="TextString" value="Last Change Date"/>
0240         <AttributeValue type="DateTime" value="2013-01-
11T00:39:11+00:00"/>
0241     </Attribute>
0242     <Attribute>
0243         <AttributeName type="TextString" value="Lease Time"/>
0244         <AttributeValue type="Interval" value="3600"/>
0245     </Attribute>
0246     <Attribute>
0247         <AttributeName type="TextString" value="Name"/>
0248         <AttributeValue>
0249             <NameValue type="TextString" value="SKLC-O-1-11"/>
0250             <NameType type="Enumeration"
value="UninterpretedTextString"/>
0251         </AttributeValue>
0252     </Attribute>
0253     <Attribute>
0254         <AttributeName type="TextString" value="State"/>
0255         <AttributeValue type="Enumeration" value="Destroyed"/>
0256     </Attribute>
0257 </ResponsePayload>
0258 </BatchItem>
0259 </ResponseMessage>

```

139

140

141 3.6 Optional Test Cases KMIP v1.2

142 3.6.1 SKLC-O-1-12

143 Create, GetAttributes, Destroy, GetAttributes

```

0001 # 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="256"/>
0021	</Attribute>
0022	<Attribute>
0023	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0024	<AttributeValue type="Integer" value="Encrypt Decrypt"/>
0025	</Attribute>
0026	<Attribute>
0027	<AttributeName type="TextString" value="Name"/>
0028	<AttributeValue>
0029	<NameValue type="TextString" value="SKLC-O-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="2012-04-27T08:12:24+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="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="$UNIQUE_IDENTIFIER_0"/>
0067     <AttributeName type="TextString" value="State"/>
0068     <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0069     <AttributeName type="TextString" value="Unique Identifier"/>
0070     <AttributeName type="TextString" value="Object Type"/>
0071     <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0072     <AttributeName type="TextString" value="Cryptographic
Length"/>
0073     <AttributeName type="TextString" value="Digest"/>
0074     <AttributeName type="TextString" value="Initial Date"/>
0075     <AttributeName type="TextString" value="Last Change Date"/>
0076     <AttributeName type="TextString" value="Activation Date"/>
0077   </RequestPayload>
0078 </BatchItem>
0079 </RequestMessage>
0080 <ResponseMessage>
0081   <ResponseHeader>
0082     <ProtocolVersion>
0083       <ProtocolVersionMajor type="Integer" value="1"/>
0084       <ProtocolVersionMinor type="Integer" value="2"/>
0085     </ProtocolVersion>
0086     <TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0087     <BatchCount type="Integer" value="1"/>
0088   </ResponseHeader>
0089   <BatchItem>
0090     <Operation type="Enumeration" value="GetAttributes"/>
0091     <ResultStatus type="Enumeration" value="Success"/>
0092     <ResponsePayload>
0093       <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0094       <Attribute>
0095         <AttributeName type="TextString" value="State"/>
0096         <AttributeValue type="Enumeration" value="PreActive"/>
0097       </Attribute>
0098       <Attribute>
0099         <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0100         <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0101       </Attribute>
0102       <Attribute>
0103         <AttributeName type="TextString" value="Unique Identifier"/>
0104         <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0105       </Attribute>
0106     </ResponsePayload>

```

0107	<AttributeName type="TextString" value="Object Type"/>
0108	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0109	</Attribute>
0110	<Attribute>
0111	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0112	<AttributeValue type="Enumeration" value="AES"/>
0113	</Attribute>
0114	<Attribute>
0115	<AttributeName type="TextString" value="Cryptographic Length"/>
0116	<AttributeValue type="Integer" value="256"/>
0117	</Attribute>
0118	<Attribute>
0119	<AttributeName type="TextString" value="Digest"/>
0120	<AttributeValue>
0121	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0122	<DigestValue type="ByteString" value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046a1b931fdaed73591f29"/>
0123	<KeyFormatType type="Enumeration" value="Raw"/>
0124	</AttributeValue>
0125	</Attribute>
0126	<Attribute>
0127	<AttributeName type="TextString" value="Initial Date"/>
0128	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0129	</Attribute>
0130	<Attribute>
0131	<AttributeName type="TextString" value="Last Change Date"/>
0132	<AttributeValue type="DateTime" value="2013-01-10T23:33:21+00:00"/>
0133	</Attribute>
0134	</ResponsePayload>
0135	</BatchItem>
0136	</ResponseMessage>
	<i># TIME 2</i>
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="Destroy"/>
0147	<RequestPayload>
0148	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0149	</RequestPayload>
0150	</BatchItem>
0151	</RequestMessage>
0152	<ResponseMessage>
0153	<ResponseHeader>
0154	<ProtocolVersion>
0155	<ProtocolVersionMajor type="Integer" value="1"/>
0156	<ProtocolVersionMinor type="Integer" value="2"/>

0157	</ProtocolVersion>
0158	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0159	<BatchCount type="Integer" value="1"/>
0160	</ResponseHeader>
0161	<BatchItem>
0162	<Operation type="Enumeration" value="Destroy"/>
0163	<ResultStatus type="Enumeration" value="Success"/>
0164	<ResponsePayload>
0165	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
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="2"/>
0174	</ProtocolVersion>
0175	<BatchCount type="Integer" value="1"/>
0176	</RequestHeader>
0177	<BatchItem>
0178	<Operation type="Enumeration" value="GetAttributes"/>
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="2012-04-27T08:12:25+00:00"/>
0191	<BatchCount type="Integer" value="1"/>
0192	</ResponseHeader>
0193	<BatchItem>
0194	<Operation type="Enumeration" value="GetAttributes"/>
0195	<ResultStatus type="Enumeration" value="Success"/>
0196	<ResponsePayload>
0197	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0198	<Attribute>
0199	<AttributeName type="TextString" value="Unique Identifier"/>
0200	<AttributeValue type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0201	</Attribute>
0202	<Attribute>
0203	<AttributeName type="TextString" value="Object Type"/>
0204	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0205	</Attribute>
0206	<Attribute>
0207	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0208	<AttributeValue type="Enumeration" value="AES"/>

```

0209     </Attribute>
0210     <Attribute>
0211         <AttributeName type="TextString" value="Cryptographic
Length"/>
0212         <AttributeValue type="Integer" value="256"/>
0213     </Attribute>
0214     <Attribute>
0215         <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0216         <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0217     </Attribute>
0218     <Attribute>
0219         <AttributeName type="TextString" value="Destroy Date"/>
0220         <AttributeValue type="DateTime" value="2013-01-
11T00:39:11+00:00"/>
0221     </Attribute>
0222     <Attribute>
0223         <AttributeName type="TextString" value="Digest"/>
0224         <AttributeValue>
0225             <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0226             <DigestValue type="ByteString"
value="bf60cac2a3f82e6added839c87b0bdbbc386d6280c14c8f09ca96e098365f7
fe3"/>
0227         <KeyFormatType type="Enumeration" value="Raw"/>
0228     </AttributeValue>
0229 </Attribute>
0230 <Attribute>
0231     <AttributeName type="TextString" value="Fresh"/>
0232     <AttributeValue type="Boolean" value="true"/>
0233 </Attribute>
0234 <Attribute>
0235     <AttributeName type="TextString" value="Initial Date"/>
0236     <AttributeValue type="DateTime" value="2013-01-
11T00:39:11+00:00"/>
0237 </Attribute>
0238 <Attribute>
0239     <AttributeName type="TextString" value="Last Change Date"/>
0240     <AttributeValue type="DateTime" value="2013-01-
11T00:39:11+00:00"/>
0241 </Attribute>
0242 <Attribute>
0243     <AttributeName type="TextString" value="Lease Time"/>
0244     <AttributeValue type="Interval" value="3600"/>
0245 </Attribute>
0246 <Attribute>
0247     <AttributeName type="TextString" value="Name"/>
0248     <AttributeValue>
0249         <NameValue type="TextString" value="SKLC-O-1-12"/>
0250         <NameType type="Enumeration"
value="UninterpretedTextString"/>
0251     </AttributeValue>
0252 </Attribute>
0253 <Attribute>
0254     <AttributeName type="TextString" value="Original Creation
Date"/>
0255     <AttributeValue type="DateTime" value="2013-01-
11T00:39:11+00:00"/>
0256 </Attribute>

```

0257	<Attribute>
0258	<AttributeName type="TextString" value="State"/>
0259	<AttributeValue type="Enumeration" value="Destroyed"/>
0260	</Attribute>
0261	</ResponsePayload>
0262	</BatchItem>
0263	</ResponseMessage>

144

145 4 Conformance

146 4.1 Symmetric Key Lifecycle Client KMIP v1.0 Profile Conformance

147 KMIP client implementations conformant to this profile:

- 148 1. SHALL support the Authentication Suite conditions (2.1) and;
- 149 2. SHALL support the Symmetric Key Lifecycle - Client conditions (2.2) and;
- 150 3. SHALL support all Mandatory Test Cases KMIP v1.0 (3.1).

151 4.2 Symmetric Key Lifecycle Client KMIP v1.1 Profile Conformance

152 KMIP client implementations conformant to this profile:

- 153 1. SHALL support the Authentication Suite conditions (2.1) and;
- 154 2. SHALL support the Symmetric Key Lifecycle - Client conditions (2.2) and;
- 155 3. SHALL support all Mandatory Test Cases KMIP v1.1 (3.2).

156 4.3 Symmetric Key Lifecycle Client KMIP v1.2 Profile Conformance

157 KMIP client implementations conformant to this profile:

- 158 1. SHALL support the Authentication Suite conditions (2.1) and;
- 159 2. SHALL support the Symmetric Key Lifecycle - Client conditions (2.2) and;
- 160 3. SHALL support all Mandatory Test Cases KMIP v1.2 (3.3).

161 4.4 Symmetric Key Lifecycle Server KMIP v1.0 Profile Conformance

162 KMIP server implementations conformant to this profile:

- 163 1. SHALL support the Authentication Suite conditions (2.1) and;
- 164 2. SHALL support the Symmetric Key Lifecycle - Server conditions (2.3) and;
- 165 3. SHALL support all Mandatory Test Cases KMIP v1.0 (3.1).

166 4.5 Symmetric Key Lifecycle Server KMIP v1.1 Profile Conformance

167 KMIP server implementations conformant to this profile:

- 168 1. SHALL support the Authentication Suite conditions (2.1) and;
- 169 2. SHALL support the Symmetric Key Lifecycle - Server conditions (2.3) and;
- 170 3. SHALL support all Mandatory Test Cases KMIP v1.1 (3.2).

171 4.6 Symmetric Key Lifecycle Server KMIP v1.2 Profile Conformance

172 KMIP server implementations conformant to this profile:

- 173 1. SHALL support the Authentication Suite conditions (2.1) and;
- 174 2. SHALL support the Symmetric Key Lifecycle - Server conditions (2.3) and;
- 175 3. SHALL support all Mandatory Test Cases KMIP v1.2 (3.3).

176 4.7 Permitted Test Case Variations

177 Whilst the test cases provided in this Profile define the allowed request and response content, some
178 inherent variations MAY occur and are permitted within a successfully completed test case.

179 Each test case MAY include allowed variations in the description of the test case in addition to the
180 variations noted in this section.

181 Other variations not explicitly noted in this Profile SHALL be deemed non-conformant.

182 4.7.1 Variable Items

183 An implementation conformant to this Profile MAY vary the following values:

- 184 1. UniqueIdentifier
- 185 2. PrivateKeyUniqueIdentifier
- 186 3. PublicKeyUniqueIdentifier
- 187 4. UniqueBatchItemIdentifier
- 188 5. AsynchronousCorrelationValue
- 189 6. TimeStamp
- 190 7. KeyValue / KeyMaterial including:
 - 191 a. key material content returned for managed cryptographic objects which are generated by
 - 192 the server
 - 193 b. wrapped versions of keys where the wrapping key is dynamic or the wrapping contains
 - 194 variable output for each wrap operation
- 195 8. For response containing the output of cryptographic operation in Data / SignatureData/ MACData
196 / IVCounterNonce where:
 - 197 a. the managed object is generated by the server; or
 - 198 b. the operation inherently contains variable output
- 199 9. For the following DateTime attributes where the value is not specified in the request as a fixed
200 DateTime value:
 - 201 a. ActivationDate
 - 202 b. ArchiveDate
 - 203 c. CompromiseDate
 - 204 d. CompromiseOccurrenceDate
 - 205 e. DeactivationDate
 - 206 f. DestroyDate
 - 207 g. InitialDate
 - 208 h. LastChangeDate
 - 209 i. ProtectStartDate
 - 210 j. ProcessStopDate
 - 211 k. ValidityDate
 - 212 l. OriginalCreationDate
- 213 10. LinkedObjectIdentifier
- 214 11. DigestValue
 - 215 a. For those managed cryptographic objects which are dynamically generated
- 216 12. KeyFormatType
 - 217 a. The key format type selected by the server when it creates managed objects
- 218 13. Digest
 - 219 a. The HashingAlgorithm selected by the server when it calculates the digest for a managed
220 object for which it has access to the key material
 - 221 b. The Digest Value

- 222 14. Extensions reported in Query for ExtensionList and ExtensionMap
- 223 15. Application Namespaces reported in Query
- 224 16. Object Types reported in Query other than those noted as required in this profile
- 225 17. Operation Types reported in Query other than those noted as required in this profile (or any
- 226 referenced profile documents)
- 227 18. For TextString attribute values containing test identifiers:
- 228 a. Additional vendor or application prefixes
- 229 19. Additional attributes beyond those noted in the response

230

231 An implementation conformant to this Profile MAY allow the following response variations:

- 232 20. Object Group values – May or may not return one or more Object Group values not included in
- 233 the requests
- 234 21. y-CustomAttributes – May or may not include additional server-specific associated attributes not
- 235 included in requests
- 236 22. Message Extensions – May or may not include additional (non-critical) vendor extensions
- 237 23. TemplateAttribute – May or may not be included in responses where the Template Attribute
- 238 response is noted as optional in [KMIP-SPEC]
- 239 24. AttributeIndex – May or may not include Attribute Index value where the Attribute Index value is 0
- 240 for Protocol Versions 1.1 and above.
- 241 25. ResultMessage – May or may not be included in responses and the value (if included) may vary
- 242 from the text contained within the test case.
- 243 26. The list of Protocol Versions returned in a DiscoverVersion response may include additional
- 244 protocol versions if the request has not specified a list of client supported Protocol Versions.
- 245 27. VendorIdentification - The value (if included) may vary from the text contained within the test
- 246 case.

247 4.7.2 Variable behavior

248 An implementation conformant to this Profile SHALL allow variation of the following behavior:

- 249 1. A test may omit the clean-up requests and responses (containing Revoke and/or Destroy) at the
- 250 end of the test provided there is a separate mechanism to remove the created objects during
- 251 testing.
- 252 2. A test may omit the test identifiers if the client is unable to include them in requests. This includes
- 253 the following attributes:
- 254 a. Name; and
- 255 b. x-ID
- 256 3. A test MAY perform requests with multiple batch items or as multiple requests with a single batch
- 257 item provided the sequence of operations are equivalent
- 258 4. A request MAY contain an optional *Authentication* [KMIP_SPEC] structure within each request
- 259

Appendix A. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

261	Hal Aldridge, Sypris Electronics
262	Mike Allen, Symantec
263	Gordon Arnold, IBM
264	Todd Arnold, IBM
265	Richard Austin, Hewlett-Packard
266	Lars Bagnert, PrimeKey
267	Elaine Barker, NIST
268	Peter Bartok, Venafi, Inc.
269	Tom Benjamin, IBM
270	Anthony Berglas, Cryptsoft
271	Mathias Björkqvist, IBM
272	Kevin Bocket, Venafi
273	Anne Bolgert, IBM
274	Alan Brown, Thales e-Security
275	Tim Bruce, CA Technologies
276	Chris Burchett, Credant Technologies, Inc.
277	Kelley Burgin, National Security Agency
278	Robert Burns, Thales e-Security
279	Chuck Castleton, Venafi
280	Kenli Chong, QuintessenceLabs
281	John Clark, Hewlett-Packard
282	Tom Clifford, Symantec Corp.
283	Doron Cohen, SafeNet, Inc
284	Tony Cox, Cryptsoft
285	Russell Dietz, SafeNet, Inc
286	Graydon Dodson, Lexmark International Inc.
287	Vinod Duggirala, EMC Corporation
288	Chris Dunn, SafeNet, Inc.
289	Michael Duren, Sypris Electronics
290	James Dzierzanowski, American Express CCoE
291	Faisal Faruqui, Thales e-Security
292	Stan Feather, Hewlett-Packard
293	David Finkelstein, Symantec Corp.
294	James Fitzgerald, SafeNet, Inc.
295	Indra Fitzgerald, Hewlett-Packard
296	Judith Furlong, EMC Corporation
297	Susan Gleeson, Oracle
298	Robert Griffin, EMC Corporation
299	Paul Grojean, Individual
300	Robert Haas, IBM
301	Thomas Hardjono, M.I.T.
302	ChengDong He, Huawei Technologies Co., Ltd.
303	Steve He, Vormetric
304	Kurt Heberlein, Hewlett-Packard
305	Larry Hofer, Emulex Corporation
306	Maryann Hondo, IBM
307	Walt Hubis, NetApp
308	Tim Hudson, Cryptsoft
309	Jonas Iggbom, Venafi, Inc.

310 Sitaram Inguva, American Express CCoE
311 Jay Jacobs, Target Corporation
312 Glen Jaquette, IBM
313 Mahadev Karadiguddi, NetApp
314 Greg Kazmierczak, Wave Systems Corp.
315 Marc Kenig, SafeNet, Inc.
316 Mark Knight, Thales e-Security
317 Kathy Kriese, Symantec Corporation
318 Mark Lambiase, SecureAuth
319 John Leiseboer, Quintessence Labs
320 Hal Lockhart, Oracle Corporation
321 Robert Lockhart, Thales e-Security
322 Anne Luk, Cryptsoft
323 Sairam Manidi, Freescale
324 Luther Martin, Voltage Security
325 Neil McEvoy, iFOSSF
326 Marina Milshtein, Individual
327 Dale Moberg, Axway Software
328 Jishnu Mukeri, Hewlett-Packard
329 Bryan Olson, Hewlett-Packard
330 John Peck, IBM
331 Rob Philpott, EMC Corporation
332 Denis Pochuev, SafeNet, Inc.
333 Reid Poole, Venafi, Inc.
334 Ajai Puri, SafeNet, Inc.
335 Saravanan Ramalingam, Thales e-Security
336 Peter Reed, SafeNet, Inc.
337 Bruce Rich, IBM
338 Christina Richards, American Express CCoE
339 Warren Robbins, Dell
340 Peter Robinson, EMC Corporation
341 Scott Rotondo, Oracle
342 Saikat Saha, SafeNet, Inc.
343 Anil Saldhana, Red Hat
344 Subhash Sankuratipati, NetApp
345 Boris Schumperli, Cryptomathic
346 Greg Singh, QuintessenceLabs
347 David Smith, Venafi, Inc
348 Brian Spector, Certivox
349 Terence Spies, Voltage Security
350 Deborah Steckroth, RouteOne LLC
351 Michael Stevens, QuintessenceLabs
352 Marcus Streets, Thales e-Security
353 Satish Sundar, IBM
354 Kiran Thota, VMware
355 Somanchi Trinath, Freescale Semiconductor, Inc.
356 Nathan Turajski, Thales e-Security
357 Sean Turner, IECA, Inc.
358 Paul Turner, Venafi, Inc.
359 Rod Wideman, Quantum Corporation
360 Steven Wierenga, Hewlett-Packard
361 Jin Wong, QuintessenceLabs
362 Sameer Yami, Thales e-Security
363 Peter Yee, EMC Corporation
364 Krishna Yellepeddy, IBM
365 Catherine Ying, SafeNet, Inc.
366 Tatu Ylonen, SSH Communications Security (Tectia Corp)

367 Michael Yoder, Vormetric. Inc.
368 Magda Zdunkiewicz, Cryptsoft
369 Peter Zelechowski, Election Systems & Software

Appendix B. KMIP Specification Cross Reference

Reference Term	KMIP 1.0	KMIP 1.1	KMIP 1.2
1 Introduction			
<i>Non-Normative References</i>	1.3.	1.3.	1.3.
<i>Normative References</i>	1.2.	1.2.	1.2.
<i>Terminology</i>	1.1.	1.1.	1.1.
2 Objects			
<i>Attribute</i>	2.1.1.	2.1.1.	2.1.1.
<i>Base Objects</i>	2.1.	2.1.	2.1.
<i>Certificate</i>	2.2.1.	2.2.1.	2.2.1.
<i>Credential</i>	2.1.2.	2.1.2.	2.1.2.
<i>Data</i>	-	-	2.1.10.
<i>Data Length</i>	-	-	2.1.11.
<i>Extension Information</i>	-	2.1.9.	2.1.9.
<i>Key Block</i>	2.1.3.	2.1.3.	2.1.3.
<i>Key Value</i>	2.1.4.	2.1.4.	2.1.4.
<i>Key Wrapping Data</i>	2.1.5.	2.1.5.	2.1.5.
<i>Key Wrapping Specification</i>	2.1.6.	2.1.6.	2.1.6.
<i>MAC Data</i>	-	-	2.1.13.
<i>Managed Objects</i>	2.2.	2.2.	2.2.
<i>Nonce</i>	-	-	2.1.14.
<i>Opaque Object</i>	2.2.8.	2.2.8.	2.2.8.
<i>PGP Key</i>	-	-	2.2.9.
<i>Private Key</i>	2.2.4.	2.2.4.	2.2.4.
<i>Public Key</i>	2.2.3.	2.2.3.	2.2.3.
<i>Secret Data</i>	2.2.7.	2.2.7.	2.2.7.
<i>Signature Data</i>	-	-	2.1.12.
<i>Split Key</i>	2.2.5.	2.2.5.	2.2.5.
<i>Symmetric Key</i>	2.2.2.	2.2.2.	2.2.2.
<i>Template</i>	2.2.6.	2.2.6.	2.2.6.
<i>Template-Attribute Structures</i>	2.1.8.	2.1.8.	2.1.8.
<i>Transparent DH Private Key</i>	2.1.7.6.	2.1.7.6.	2.1.7.6.
<i>Transparent DH Public Key</i>	2.1.7.7.	2.1.7.7.	2.1.7.7.
<i>Transparent DSA Private Key</i>	2.1.7.2.	2.1.7.2.	2.1.7.2.
<i>Transparent DSA Public Key</i>	2.1.7.3.	2.1.7.3.	2.1.7.3.
<i>Transparent ECDH Private Key</i>	2.1.7.10.	2.1.7.10.	2.1.7.10.
<i>Transparent ECDH Public Key</i>	2.1.7.11.	2.1.7.11.	2.1.7.11.
<i>Transparent ECDSA Private Key</i>	2.1.7.8.	2.1.7.8.	2.1.7.8.
<i>Transparent ECDSA Public Key</i>	2.1.7.9.	2.1.7.9.	2.1.7.9.
<i>Transparent ECMQV Private Key</i>	2.1.7.12.	2.1.7.12.	2.1.7.12.
<i>Transparent ECMQV Public Key</i>	2.1.7.13.	2.1.7.13.	2.1.7.13.
<i>Transparent Key Structures</i>	2.1.7.	2.1.7.	2.1.7.
<i>Transparent RSA Private Key</i>	2.1.7.4.	2.1.7.4.	2.1.7.4.
<i>Transparent RSA Public Key</i>	2.1.7.5.	2.1.7.5.	2.1.7.5.
<i>Transparent Symmetric Key</i>	2.1.7.1.	2.1.7.1.	2.1.7.1.
3 Attributes			
<i>Activation Date</i>	3.19.	3.24.	3.24.
<i>Alternative Name</i>	-	-	3.40.
<i>Application Specific Information</i>	3.30.	3.36.	3.36.
<i>Archive Date</i>	3.27.	3.32.	3.32.

Reference Term	KMIP 1.0	KMIP 1.1	KMIP 1.2
<i>Attributes</i>	3	3	3
<i>Certificate Identifier</i>	3.9.	3.13.	3.13.
<i>Certificate Issuer</i>	3.11.	3.15.	3.15.
<i>Certificate Length</i>	-	3.9.	3.9.
<i>Certificate Subject</i>	3.10.	3.14.	3.14.
<i>Certificate Type</i>	3.8.	3.8.	3.8.
<i>Compromise Date</i>	3.25.	3.30.	3.30.
<i>Compromise Occurrence Date</i>	3.24.	3.29.	3.29.
<i>Contact Information</i>	3.31.	3.37.	3.37.
<i>Cryptographic Algorithm</i>	3.4.	3.4.	3.4.
<i>Cryptographic Domain Parameters</i>	3.7.	3.7.	3.7.
<i>Cryptographic Length</i>	3.5.	3.5.	3.5.
<i>Cryptographic Parameters</i>	3.6.	3.6.	3.6.
<i>Custom Attribute</i>	3.33.	3.39.	3.39.
<i>Deactivation Date</i>	3.22.	3.27.	3.27.
<i>Default Operation Policy</i>	3.13.2.	3.18.2.	3.18.2.
<i>Default Operation Policy for Certificates and Public Key Objects</i>	3.13.2.2.	3.18.2.2.	3.18.2.2.
<i>Default Operation Policy for Secret Objects</i>	3.13.2.1.	3.18.2.1.	3.18.2.1.
<i>Default Operation Policy for Template Objects</i>	3.13.2.3.	3.18.2.3.	3.18.2.3.
<i>Destroy Date</i>	3.23.	3.28.	3.28.
<i>Digest</i>	3.12.	3.17.	3.17.
<i>Digital Signature Algorithm</i>	-	3.16.	3.16.
<i>Fresh</i>	-	3.34.	3.34.
<i>Initial Date</i>	3.18.	3.23.	3.23.
<i>Key Value Location</i>	-	-	3.42.
<i>Key Value Present</i>	-	-	3.41.
<i>Last Change Date</i>	3.32.	3.38.	3.38.
<i>Lease Time</i>	3.15.	3.20.	3.20.
<i>Link</i>	3.29.	3.35.	3.35.
<i>Name</i>	3.2.	3.2.	3.2.
<i>Object Group</i>	3.28.	3.33.	3.33.
<i>Object Type</i>	3.3.	3.3.	3.3.
<i>Operation Policy Name</i>	3.13.	3.18.	3.18.
<i>Operations outside of operation policy control</i>	3.13.1.	3.18.1.	3.18.1.
<i>Original Creation Date</i>	-	-	3.43.
<i>Process Start Date</i>	3.20.	3.25.	3.25.
<i>Protect Stop Date</i>	3.21.	3.26.	3.26.
<i>Revocation Reason</i>	3.26.	3.31.	3.31.
<i>State</i>	3.17.	3.22.	3.22.
<i>Unique Identifier</i>	3.1.	3.1.	3.1.
<i>Usage Limits</i>	3.16.	3.21.	3.21.
<i>X.509 Certificate Identifier</i>	-	3.10.	3.10.
<i>X.509 Certificate Issuer</i>	-	3.12.	3.12.
<i>X.509 Certificate Subject</i>	-	3.11.	3.11.
4 Client-to-Server Operations			
<i>Activate</i>	4.18.	4.19.	4.19.
<i>Add Attribute</i>	4.13.	4.14.	4.14.
<i>Archive</i>	4.21.	4.22.	4.22.
<i>Cancel</i>	4.25.	4.27.	4.27.
<i>Certify</i>	4.6.	4.7.	4.7.
<i>Check</i>	4.9.	4.10.	4.10.
<i>Create</i>	4.1.	4.1.	4.1.
<i>Create Key Pair</i>	4.2.	4.2.	4.2.

Reference Term	KMIP 1.0	KMIP 1.1	KMIP 1.2
<i>Create Split Key</i>	-	-	4.38.
<i>Decrypt</i>	-	-	4.30.
<i>Delete Attribute</i>	4.15.	4.16.	4.16.
<i>Derive Key</i>	4.5.	4.6.	4.6.
<i>Destroy</i>	4.20.	4.21.	4.21.
<i>Discover Versions</i>	-	4.26.	4.26.
<i>Encrypt</i>	-	-	4.29.
<i>Get</i>	4.10.	4.11.	4.11.
<i>Get Attribute List</i>	4.12.	4.13.	4.13.
<i>Get Attributes</i>	4.11.	4.12.	4.12.
<i>Get Usage Allocation</i>	4.17.	4.18.	4.18.
<i>Hash</i>	-	-	4.37.
<i>Join Split Key</i>	-	-	4.39.
<i>Locate</i>	4.8.	4.9.	4.9.
<i>MAC</i>	-	-	4.33.
<i>MAC Verify</i>	-	-	4.34.
<i>Modify Attribute</i>	4.14.	4.15.	4.15.
<i>Obtain Lease</i>	4.16.	4.17.	4.17.
<i>Poll</i>	4.26.	4.28.	4.28.
<i>Query</i>	4.24.	4.25.	4.25.
<i>Re-certify</i>	4.7.	4.8.	4.8.
<i>Recover</i>	4.22.	4.23.	4.23.
<i>Register</i>	4.3.	4.3.	4.3.
<i>Re-key</i>	4.4.	4.4.	4.4.
<i>Re-key Key Pair</i>	-	4.5.	4.5.
<i>Revoke</i>	4.19.	4.20.	4.20.
<i>RNG Retrieve</i>	-	-	4.35.
<i>RNG Seed</i>	-	-	4.36.
<i>Sign</i>	-	-	4.31.
<i>Signature Verify</i>	-	-	4.32.
<i>Validate</i>	4.23.	4.24.	4.24.
5 Server-to-Client Operations			
<i>Notify</i>	5.1.	5.1.	5.1.
<i>Put</i>	5.2.	5.2.	5.2.
6 Message Contents			
<i>Asynchronous Correlation Value</i>	6.8.	6.8.	6.8.
<i>Asynchronous Indicator</i>	6.7.	6.7.	6.7.
<i>Attestation Capable Indicator</i>	-	-	6.17.
<i>Batch Count</i>	6.14.	6.14.	6.14.
<i>Batch Error Continuation Option</i>	6.13.	6.13.	6.13.
<i>Batch Item</i>	6.15.	6.15.	6.15.
<i>Batch Order Option</i>	6.12.	6.12.	6.12.
<i>Maximum Response Size</i>	6.3.	6.3.	6.3.
<i>Message Extension</i>	6.16.	6.16.	6.16.
<i>Operation</i>	6.2.	6.2.	6.2.
<i>Protocol Version</i>	6.1.	6.1.	6.1.
<i>Result Message</i>	6.11.	6.11.	6.11.
<i>Result Reason</i>	6.10.	6.10.	6.10.
<i>Result Status</i>	6.9.	6.9.	6.9.
<i>Time Stamp</i>	6.5.	6.5.	6.5.
<i>Unique Batch Item ID</i>	6.4.	6.4.	6.4.
7 Message Format			

Reference Term	KMIP 1.0	KMIP 1.1	KMIP 1.2
<i>Message Structure</i>	7.1.	7.1.	7.1.
<i>Operations</i>	7.2.	7.2.	7.2.
8 Authentication			
<i>Authentication</i>	8	8	8
9 Message Encoding			
<i>Alternative Name Type Enumeration</i>	-	-	9.1.3.2.34.
<i>Attestation Type Enumeration</i>	-	-	9.1.3.2.36.
<i>Batch Error Continuation Option Enumeration</i>	9.1.3.2.29.	9.1.3.2.30.	9.1.3.2.30.
<i>Bit Masks</i>	9.1.3.3.	9.1.3.3.	9.1.3.3.
<i>Block Cipher Mode Enumeration</i>	9.1.3.2.13.	9.1.3.2.14.	9.1.3.2.14.
<i>Cancellation Result Enumeration</i>	9.1.3.2.24.	9.1.3.2.25.	9.1.3.2.25.
<i>Certificate Request Type Enumeration</i>	9.1.3.2.21.	9.1.3.2.22.	9.1.3.2.22.
<i>Certificate Type Enumeration</i>	9.1.3.2.6.	9.1.3.2.6.	9.1.3.2.6.
<i>Credential Type Enumeration</i>	9.1.3.2.1.	9.1.3.2.1.	9.1.3.2.1.
<i>Cryptographic Algorithm Enumeration</i>	9.1.3.2.12.	9.1.3.2.13.	9.1.3.2.13.
<i>Cryptographic Usage Mask</i>	9.1.3.3.1.	9.1.3.3.1.	9.1.3.3.1.
<i>Defined Values</i>	9.1.3.	9.1.3.	9.1.3.
<i>Derivation Method Enumeration</i>	9.1.3.2.20.	9.1.3.2.21.	9.1.3.2.21.
<i>Digital Signature Algorithm Enumeration</i>	-	9.1.3.2.7.	9.1.3.2.7.
<i>Encoding Option Enumeration</i>	-	9.1.3.2.32.	9.1.3.2.32.
<i>Enumerations</i>	9.1.3.2.	9.1.3.2.	9.1.3.2.
<i>Examples</i>	9.1.2.	9.1.2.	9.1.2.
<i>Hashing Algorithm Enumeration</i>	9.1.3.2.15.	9.1.3.2.16.	9.1.3.2.16.
<i>Item Length</i>	9.1.1.3.	9.1.1.3.	9.1.1.3.
<i>Item Tag</i>	9.1.1.1.	9.1.1.1.	9.1.1.1.
<i>Item Type</i>	9.1.1.2.	9.1.1.2.	9.1.1.2.
<i>Item Value</i>	9.1.1.4.	9.1.1.4.	9.1.1.4.
<i>Key Compression Type Enumeration</i>	9.1.3.2.2.	9.1.3.2.2.	9.1.3.2.2.
<i>Key Format Type Enumeration</i>	9.1.3.2.3.	9.1.3.2.3.	9.1.3.2.3.
<i>Key Role Type Enumeration</i>	9.1.3.2.16.	9.1.3.2.17.	9.1.3.2.17.
<i>Key Value Location Type Enumeration</i>	-	-	9.1.3.2.35.
<i>Link Type Enumeration</i>	9.1.3.2.19.	9.1.3.2.20.	9.1.3.2.20.
<i>Name Type Enumeration</i>	9.1.3.2.10.	9.1.3.2.11.	9.1.3.2.11.
<i>Object Group Member Enumeration</i>	-	9.1.3.2.33.	9.1.3.2.33.
<i>Object Type Enumeration</i>	9.1.3.2.11.	9.1.3.2.12.	9.1.3.2.12.
<i>Opaque Data Type Enumeration</i>	9.1.3.2.9.	9.1.3.2.10.	9.1.3.2.10.
<i>Operation Enumeration</i>	9.1.3.2.26.	9.1.3.2.27.	9.1.3.2.27.
<i>Padding Method Enumeration</i>	9.1.3.2.14.	9.1.3.2.15.	9.1.3.2.15.
<i>Put Function Enumeration</i>	9.1.3.2.25.	9.1.3.2.26.	9.1.3.2.26.
<i>Query Function Enumeration</i>	9.1.3.2.23.	9.1.3.2.24.	9.1.3.2.24.
<i>Recommended Curve Enumeration for ECDSA, ECDH, and ECMQV</i>	9.1.3.2.5.	9.1.3.2.5.	9.1.3.2.5.
<i>Result Reason Enumeration</i>	9.1.3.2.28.	9.1.3.2.29.	9.1.3.2.29.
<i>Result Status Enumeration</i>	9.1.3.2.27.	9.1.3.2.28.	9.1.3.2.28.
<i>Revocation Reason Code Enumeration</i>	9.1.3.2.18.	9.1.3.2.19.	9.1.3.2.19.
<i>Secret Data Type Enumeration</i>	9.1.3.2.8.	9.1.3.2.9.	9.1.3.2.9.
<i>Split Key Method Enumeration</i>	9.1.3.2.7.	9.1.3.2.8.	9.1.3.2.8.
<i>State Enumeration</i>	9.1.3.2.17.	9.1.3.2.18.	9.1.3.2.18.
<i>Storage Status Mask</i>	9.1.3.3.2.	9.1.3.3.2.	9.1.3.3.2.
<i>Tags</i>	9.1.3.1.	9.1.3.1.	9.1.3.1.
<i>TTLV Encoding</i>	9.1.	9.1.	9.1.
<i>TTLV Encoding Fields</i>	9.1.1.	9.1.1.	9.1.1.
<i>Usage Limits Unit Enumeration</i>	9.1.3.2.30.	9.1.3.2.31.	9.1.3.2.31.

Reference Term	KMIP 1.0	KMIP 1.1	KMIP 1.2
<i>Validity Indicator Enumeration</i>	9.1.3.2.22.	9.1.3.2.23.	9.1.3.2.23.
<i>Wrapping Method Enumeration</i>	9.1.3.2.4.	9.1.3.2.4.	9.1.3.2.4.
<i>XML Encoding</i>	9.2.	-	-
10 Transport			
<i>Transport</i>	10	10	10
12 KMIP Server and Client Implementation Conformance			
<i>Conformance clauses for a KMIP Server</i>	12.1.	-	-
<i>KMIP Client Implementation Conformance</i>	-	12.2.	12.2.
<i>KMIP Server Implementation Conformance</i>	-	12.1.	12.1.

370

371

Appendix C. Revision History

372

Revision	Date	Editor	Changes Made
wd01	26-June-2013	Tim Hudson / Bob Lockhart	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 / Bob Lockhart	Updated to include Permitted Test Case Variations and updated Test Cases based on July 2013 Interop
wd03	10-August-2013	Tim Hudson	Updated Permitted Test Case Variations and corrected Protect Stop Date typographic error in 2.2
wd03a	24-October- 2013	Tim Hudson	Editorial update to include VendorIdentification in the list of allowed variations as per TC motion.
pr01update	11-June-2014	Tim Hudson	Updated following Public Review

373