

KMIP Symmetric Key Lifecycle Profile Version 1.0

Committee Specification Draft 01

31 October 2013

Specification URIs

This version:

<http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/csd01/kmip-sym-key-profile-v1.0-csd01.doc> (Authoritative)
<http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/csd01/kmip-sym-key-profile-v1.0-csd01.html>
<http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/csd01/kmip-sym-key-profile-v1.0-csd01.pdf>

Previous version:

N/A

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:

Robert Griffin (robert.griffin@rsa.com), EMC Corporation
Subhash Sankuratripati (Subhash.Sankuratripati@netapp.com), NetApp

Editors:

Tim Hudson (tjh@cryptsoft.com), Cryptsoft Pty Ltd.
Robert Lockhart (Robert.Lockhart@thalessec.com), Thales e-Security

Related work:

This specification is related to:

- *Key Management Interoperability Protocol Profiles Version 1.0*. 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*. Latest version. <http://docs.oasis-open.org/kmip/spec/v1.1/kmip-spec-v1.1.html>.
- *Key Management Interoperability Protocol Specification Version 1.2*. 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 <http://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 (<http://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. 31 October 2013. OASIS Committee Specification Draft 01. <http://docs.oasis-open.org/kmip/kmip-sym-key-profile/v1.0/csd01/kmip-sym-key-profile-v1.0-csd01.html>.

Notices

Copyright © OASIS Open 2013. 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 <http://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
1.3	Non-Normative References	5
2	Symmetric Key Lifecycle Profile	7
2.1	Authentication Suite	7
2.2	Baseline	7
3	Symmetric Key Lifecycle Profile - Test Cases	8
3.1	Mandatory Test Cases KMIP 1.0	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 1.1	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 1.2	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 1.0	59
3.4.1	SKLC-O-1-10	59
3.5	Optional Test Cases KMIP 1.1	64
3.5.1	SKLC-O-1-11	64
3.6	Optional Test Cases KMIP 1.2	69
3.6.1	SKLC-O-1-12	70
4	Symmetric Key Lifecycle Profile - Test Cases	76
4.1	Mandatory Test Cases	76
5	Conformance	77
5.1	Conformance Statement	77
5.2	Permitted Test Case Variations	77
5.2.1	Variable Items	77
5.2.2	Variable behavior	78
Appendix A.	Acknowledgments	80
Appendix B.	KMIP Specification Cross Reference	83
Appendix C.	Revision History	88

1 Introduction

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

Illustrative guidance for the implementation of KMIP clients and servers is provided in the [KMIP Usage Guide](#) [KMIP-UG].

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>.
- [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>.
- [RFC2246] T. Dierks and C. Allen, *The TLS Protocol, Version 1.0*, IETF RFC 2246, Jan 1999, <http://www.ietf.org/rfc/rfc2246.txt>
- [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 Usage Guide 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 Usage Guide 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 Usage Guide Version 1.2.*
[URL](#)
Candidate OASIS Standard 01. DD MMM YYYY.

1.3 Non-Normative References

- [KMIP-UG] One or more of [KMIP-UG-1_0], [KMIP-UG-1_1], [KMIP-UG-1_2]
- [KMIP-UG-1_0] *Key Management Interoperability Protocol Usage Guide Version 1.0.*
<http://docs.oasis-open.org/kmip/ug/v1.1/kmip-ug-v1.1-cnd01.doc>
Committee Note Draft, 1 December 2011

44 **[KMIP-UG-1_1]** *Key Management Interoperability Protocol Usage Guide Version 1.1.*
45 <http://docs.oasis-open.org/kmip/ug/v1.1/cn01/kmip-ug-v1.1-cn01.doc>
46 Committee Note 01, 27 July 2012
47 **[KMIP-UG-1_2]** *Key Management Interoperability Protocol Usage Guide Version 1.2.*
48 URL
49 Committee Note Draft, DD MMM YYYY
50 **[KMIP-TC-1_1]** *Key Management Interoperability Protocol Test Cases Version 1.1.*
51 [http://docs.oasis-open.org/kmip/testcases/v1.1/cn01/kmip-testcases-v1.1-](http://docs.oasis-open.org/kmip/testcases/v1.1/cn01/kmip-testcases-v1.1-cn01.doc)
52 cn01.doc, Committee Note 01, 27 July 2012.
53 **[KMIP-TC-1_2]** *Key Management Interoperability Protocol Test Cases Version 1.2.*
54 URL, Committee Note Draft, DD MMM YYYY.
55 **[KMIP-UC]** *Key Management Interoperability Protocol Use Cases Version 1.0.*
56 [http://docs.oasis-open.org/kmip/usecases/v1.0/cs01/kmip-usecases-1.0-cs-](http://docs.oasis-open.org/kmip/usecases/v1.0/cs01/kmip-usecases-1.0-cs-01.doc)
57 01.doc, Committee Specification, 15 June 2010.

2 Symmetric Key Lifecycle Profile

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

2.1 Authentication Suite

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

2.2 Baseline

KMIP clients conformant to this profile:

1. SHALL conform to the KMIP Baseline Client profile in [KMIP-PROF] and [KMIP-SPEC]

KMIP servers conformant to this profile:

1. SHALL conform to the KMIP Baseline Server profile in [KMIP-PROF] and [KMIP-SPEC] and
2. SHALL support the following *Objects* [KMIP-SPEC]
 - a. *Symmetric Key* [KMIP-SPEC]
 - b. *Key Format Type* [KMIP-SPEC]
3. SHALL support the following *Attributes* [KMIP-SPEC]
 - a. *Cryptographic Algorithm* [KMIP-SPEC]
 - b. *Object Type* [KMIP-SPEC]
 - c. *Process Start Date* [KMIP-SPEC]
 - d. *Protect Stop Date* [KMIP-SPEC]
4. SHALL support the following *Client-to-Server* [KMIP-SPEC] operations:
 - a. *Create* [KMIP-SPEC]
5. SHALL support the following *Message Encoding* [KMIP-SPEC]:
 - a. *Cryptographic Algorithm* [KMIP-SPEC] with values:
 - i. 3DES
 - ii. AES
 - b. *Object Type* [KMIP-SPEC] with value:
 - i. Symmetric Key
 - c. *Key Format Type* [KMIP-SPEC] with value:
 - i. Raw
 - ii. Transparent Symmetric Key
6. SHALL support all Mandatory Test Cases, returning results in accordance with the test cases.
7. MAY support any clause within [KMIP-SPEC] provided it does not conflict with any other clause within this section 2.2
8. MAY support extensions outside the scope of this standard (e.g., vendor extensions, conformance clauses) that do not contradict any KMIP requirements.

3 Symmetric Key Lifecycle Profile - Test Cases

This section documents the test cases for a KMIP server performing symmetric key lifecycle operations based on requests received from a KMIP client.

Note: the values for the returned items and the custom attributes are illustrative. Actual values from a real client system will vary.

3.1 Mandatory Test Cases KMIP 1.0

This section documents the test cases that a client or server conformant to the Symmetric Key Lifecycle Profile SHALL support under KMIP Specification 1.0.

3.1.1 SKLC-M-1-10

Create, 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-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"
0052	value="\$UNIQUE_IDENTIFIER_0"/>
0053	</ResponsePayload>
0054	</BatchItem>
0055	</ResponseMessage>
# TIME 1	
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="0"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="GetAttributes"/>
0065	<RequestPayload>
0066	<UniqueIdentifier type="TextString"
0067	value="\$UNIQUE_IDENTIFIER_0"/>
0068	<AttributeName type="TextString" value="State"/>
0069	<AttributeName type="TextString" value="Cryptographic Usage
0070	Mask"/>
0071	<AttributeName type="TextString" value="Unique Identifier"/>
0072	<AttributeName type="TextString" value="Object Type"/>
0073	<AttributeName type="TextString" value="Cryptographic
0074	Algorithm"/>
0075	<AttributeName type="TextString" value="Cryptographic
0076	Length"/>
0077	<AttributeName type="TextString" value="Digest"/>
0078	<AttributeName type="TextString" value="Initial Date"/>
0079	<AttributeName type="TextString" value="Last Change Date"/>
0080	<AttributeName type="TextString" value="Activation Date"/>
0081	</RequestPayload>
0082	</BatchItem>
0083	</RequestMessage>
0084	<ResponseMessage>
0085	<ResponseHeader>
0086	<ProtocolVersion>
	<ProtocolVersionMajor type="Integer" value="1"/>
	<ProtocolVersionMinor type="Integer" value="0"/>
	</ProtocolVersion>
	<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             </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="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>

104

105 3.1.2 SKLC-M-2-10

106 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
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>
	<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>
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="Destroy"/>
0220	<RequestPayload>
0221	<UniqueIdentifier type="TextString"

0222	value="\$UNIQUE_IDENTIFIER_0"/>
0223	</RequestPayload>
0224	</BatchItem>
0225	</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>
0277	# TIME 6
0278	<RequestMessage>
0279	<RequestHeader>
0280	<ProtocolVersion>
0281	<ProtocolVersionMajor type="Integer" value="1"/>
0282	<ProtocolVersionMinor type="Integer" value="0"/>
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="0"/>
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>
0315	# TIME 7
0316	<RequestMessage>
0317	<RequestHeader>
0318	<ProtocolVersion>
0319	<ProtocolVersionMajor type="Integer" value="1"/>
0320	<ProtocolVersionMinor type="Integer" value="0"/>
0321	</ProtocolVersion>
0322	<BatchCount type="Integer" value="1"/>
0323	</RequestHeader>
0324	<BatchItem>
0325	<Operation type="Enumeration" value="Destroy"/>
0326	<RequestPayload>
0327	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0328	</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>

107

108 3.1.3 SKLC-M-3-10

109 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>
	# TIME 1
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="0"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="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"
0093 value="$UNIQUE_IDENTIFIER_0"/>
0094             <Attribute>
0095                 <AttributeName type="TextString" value="State"/>
0096                 <AttributeValue type="Enumeration" value="PreActive"/>
0097             </Attribute>
0098             <Attribute>
0099                 <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0100                 <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0101             </Attribute>
0102             <Attribute>
0103                 <AttributeName type="TextString" value="Unique Identifier"/>
0104                 <AttributeValue type="TextString"
0105 value="$UNIQUE_IDENTIFIER_0"/>
0106             </Attribute>
0107             <Attribute>
0108                 <AttributeName type="TextString" value="Object Type"/>
0109                 <AttributeValue type="Enumeration" value="SymmetricKey"/>
0110             </Attribute>
0111             <Attribute>
0112                 <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0113                 <AttributeValue type="Enumeration" value="AES"/>
0114             </Attribute>
0115             <Attribute>
0116                 <AttributeName type="TextString" value="Cryptographic
Length"/>
0117                 <AttributeValue type="Integer" value="256"/>
0118             </Attribute>
0119             <Attribute>
0120                 <AttributeName type="TextString" value="Digest"/>
0121                 <AttributeValue>
0122                     <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0123                     <DigestValue type="ByteString"
0124 value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046a1b931fdaed73591
f29"/>
0125                 </AttributeValue>
0126             </Attribute>
0127             <Attribute>
0128                 <AttributeName type="TextString" value="Initial Date"/>
0129                 <AttributeValue type="DateTime" value="2013-01-
10T23:33:21+00:00"/>
0130             </Attribute>
0131             <Attribute>
0132                 <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>
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>

```

110

111 3.2 Mandatory Test Cases KMIP 1.1

112 This section documents the test cases that a client or server conformant to the Symmetric Key Lifecycle
113 Profile SHALL support under KMIP Specification 1.1.

114 3.2.1 SKLC-M-1-11

115 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>
0055	# TIME 1
0056	<RequestMessage>
0057	<RequestHeader>
0058	<ProtocolVersion>
0059	<ProtocolVersionMajor type="Integer" value="1"/>
0060	<ProtocolVersionMinor type="Integer" value="1"/>
0061	</ProtocolVersion>
0062	<BatchCount type="Integer" value="1"/>
0063	</RequestHeader>
0064	<BatchItem>
0065	<Operation type="Enumeration" value="GetAttributes"/>
0066	<RequestPayload>
0067	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0068	<AttributeName type="TextString" value="State"/>
0069	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0070	<AttributeName type="TextString" value="Unique Identifier"/>
0071	<AttributeName type="TextString" value="Object Type"/>
0072	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0073	<AttributeName type="TextString" value="Cryptographic Length"/>
0074	<AttributeName type="TextString" value="Digest"/>
0075	<AttributeName type="TextString" value="Initial Date"/>
0076	<AttributeName type="TextString" value="Last Change Date"/>
0077	<AttributeName type="TextString" value="Activation Date"/>
0078	</RequestPayload>
0079	</BatchItem>
0080	</RequestMessage>
0081	<ResponseMessage>
0082	<ResponseHeader>
0083	<ProtocolVersion>
	<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="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>
# 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>

116

117 3.2.2 SKLC-M-2-11

118 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
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	</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

0115	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"/>
	<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="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>
# TIME 3	
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="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>
	# TIME 5
0242	<RequestMessage>
0243	<RequestHeader>
0244	<ProtocolVersion>
0245	<ProtocolVersionMajor type="Integer" value="1"/>
0246	<ProtocolVersionMinor type="Integer" value="1"/>
0247	</ProtocolVersion>
0248	<BatchCount type="Integer" value="1"/>
0249	</RequestHeader>
0250	<BatchItem>
0251	<Operation type="Enumeration" value="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>

119

120 3.2.3 SKLC-M-3-11

121 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
0056	<RequestMessage>
0057	<RequestHeader>
0058	<ProtocolVersion>
0059	<ProtocolVersionMajor type="Integer" value="1"/>
0060	<ProtocolVersionMinor type="Integer" value="1"/>
0061	</ProtocolVersion>
0062	<BatchCount type="Integer" value="1"/>
0063	</RequestHeader>
0064	<BatchItem>
0065	<Operation type="Enumeration" value="GetAttributes"/>
0066	<RequestPayload>
	<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>
# TIME 2	
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>
# TIME 3	
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"
	value="\$UNIQUE_IDENTIFIER_0"/>
0281	</ResponsePayload>
0282	</BatchItem>
0283	</ResponseMessage>

0284	# TIME 6
0285	<RequestMessage>
0286	<RequestHeader>
0287	<ProtocolVersion>
0288	<ProtocolVersionMajor type="Integer" value="1"/>
0289	<ProtocolVersionMinor type="Integer" value="1"/>
0290	</ProtocolVersion>
0291	<BatchCount type="Integer" value="1"/>
0292	</RequestHeader>
0293	<BatchItem>
0294	<Operation type="Enumeration" value="GetAttributes"/>
0295	<RequestPayload>
0296	<UniqueIdentifier type="TextString"
0297	value="\$UNIQUE_IDENTIFIER_0"/>
0298	<AttributeName type="TextString" value="State"/>
0299	</RequestPayload>
0300	</BatchItem>
0301	</RequestMessage>
0302	<ResponseMessage>
0303	<ResponseHeader>
0304	<ProtocolVersion>
0305	<ProtocolVersionMajor type="Integer" value="1"/>
0306	<ProtocolVersionMinor type="Integer" value="1"/>
0307	</ProtocolVersion>
0308	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0309	<BatchCount type="Integer" value="1"/>
0310	</ResponseHeader>
0311	<BatchItem>
0312	<Operation type="Enumeration" value="GetAttributes"/>
0313	<ResultStatus type="Enumeration" value="Success"/>
0314	<ResponsePayload>
0315	<UniqueIdentifier type="TextString"
0316	value="\$UNIQUE_IDENTIFIER_0"/>
0317	<Attribute>
0318	<AttributeName type="TextString" value="State"/>
0319	<AttributeValue type="Enumeration" value="Compromised"/>
0320	</Attribute>
0321	</ResponsePayload>
0322	</BatchItem>
0323	</ResponseMessage>
0324	# TIME 7
0325	<RequestMessage>
0326	<RequestHeader>
0327	<ProtocolVersion>
0328	<ProtocolVersionMajor type="Integer" value="1"/>
0329	<ProtocolVersionMinor type="Integer" value="1"/>
0330	</ProtocolVersion>
0331	<BatchCount type="Integer" value="1"/>
0332	</RequestHeader>
0333	<BatchItem>
0334	<Operation type="Enumeration" value="Destroy"/>
0335	<RequestPayload>
0336	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
	</RequestPayload>
	</BatchItem>
	</RequestMessage>
	<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"
0350 value="$UNIQUE_IDENTIFIER_0"/>
0351   </ResponsePayload>
0352 </BatchItem>
</ResponseMessage>

```

122

123 3.3 Mandatory Test Cases KMIP 1.2

124 This section documents the test cases that a client or server conformant to the Symmetric Key Lifecycle
125 Profile SHALL support under KMIP Specification 1.2.

126 3.3.1 SKLC-M-1-12

127 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       </TemplateAttribute>

```

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>
	# TIME 1
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="2"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="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"
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="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046alb931fdaed73591f29"/>
	</AttributeValue>
	</Attribute>
	<Attribute>
	<AttributeName type="TextString" value="Initial Date"/>
	<AttributeValue type="DateTime" value="2013-01-

0129	10T23:33:21+00:00"/>
0130	</Attribute>
0131	<Attribute 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
0138	<RequestMessage>
0139	<RequestHeader>
0140	<ProtocolVersion>
0141	<ProtocolVersionMajor type="Integer" value="1"/>
0142	<ProtocolVersionMinor type="Integer" value="2"/>
0143	</ProtocolVersion>
0144	<BatchCount type="Integer" value="1"/>
0145	</RequestHeader>
0146	<BatchItem>
0147	<Operation type="Enumeration" value="Destroy"/>
0148	<RequestPayload>
0149	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0150	</RequestPayload>
0151	</BatchItem>
0152	</RequestMessage>
0153	<ResponseMessage>
0154	<ResponseHeader>
0155	<ProtocolVersion>
0156	<ProtocolVersionMajor type="Integer" value="1"/>
0157	<ProtocolVersionMinor type="Integer" value="2"/>
0158	</ProtocolVersion>
0159	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0160	<BatchCount type="Integer" value="1"/>
0161	</ResponseHeader>
0162	<BatchItem>
0163	<Operation type="Enumeration" value="Destroy"/>
0164	<ResultStatus type="Enumeration" value="Success"/>
0165	<ResponsePayload>
0166	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0167	</ResponsePayload>
0168	</BatchItem>
0169	</ResponseMessage>

128

129 3.3.2 SKLC-M-2-12

130 Create, GetAttributes, Activate, GetAttributes, Destroy, Revoke, GetAttributes, Destroy

0001	# TIME 0
0002	<RequestMessage>
0003	<RequestHeader>
0004	<ProtocolVersion>
0005	<ProtocolVersionMajor type="Integer" value="1"/>
0006	<ProtocolVersionMinor type="Integer" value="2"/>
0007	</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>
	# TIME 1
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>

0059	<ProtocolVersionMinor type="Integer" value="2"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="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
0111	Algorithm"/>
0112	<AttributeValue type="Enumeration" value="AES"/>
0113	</Attribute>
0114	<AttributeName type="TextString" value="Cryptographic
0115	Length"/>
0116	<AttributeValue type="Integer" value="256"/>
0117	</Attribute>
0118	<AttributeName type="TextString" value="Digest"/>
0119	<AttributeValue>
0120	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0121	<DigestValue type="ByteString"
0122	value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046alb931fdaed73591
0123	f29"/>
0124	<KeyFormatType type="Enumeration" value="Raw"/>
0125	</AttributeValue>
0126	</Attribute>
0127	<AttributeName type="TextString" value="Initial Date"/>
0128	<AttributeValue type="DateTime" value="2013-01-
0129	10T23:33:21+00:00"/>
0130	</Attribute>
0131	<AttributeName type="TextString" value="Last Change Date"/>
0132	<AttributeValue type="DateTime" value="2013-01-
0133	10T23:33:21+00:00"/>
0134	</Attribute>
0135	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>
0136	# TIME 2
0137	<RequestMessage>
0138	<RequestHeader>
0139	<ProtocolVersion>
0140	<ProtocolVersionMajor type="Integer" value="1"/>
0141	<ProtocolVersionMinor type="Integer" value="2"/>
0142	</ProtocolVersion>
0143	<BatchCount type="Integer" value="1"/>
0144	</RequestHeader>
0145	<BatchItem>
0146	<Operation type="Enumeration" value="Activate"/>
0147	<RequestPayload>
0148	<UniqueIdentifier type="TextString"
0149	value="\$UNIQUE_IDENTIFIER_0"/>
0150	</RequestPayload>
0151	</BatchItem>
0152	</RequestMessage>
0153	<ResponseMessage>
0154	<ResponseHeader>
0155	<ProtocolVersion>
0156	<ProtocolVersionMajor type="Integer" value="1"/>
0157	<ProtocolVersionMinor type="Integer" value="2"/>
0158	</ProtocolVersion>
0159	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
	<BatchCount type="Integer" value="1"/>
	</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-
	01T00:00:00+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>

131

132 3.3.3 SKLC-M-3-12

133 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

0020	Length"/>
0021	<AttributeValue type="Integer" value="256"/>
0022	</Attribute>
0023	<Attribute>
0024	<AttributeName type="TextString" value="Cryptographic
0025	Usage Mask"/>
0026	<AttributeValue type="Integer" value="Encrypt Decrypt"/>
0027	</Attribute>
0028	<Attribute>
0029	<AttributeName type="TextString" value="Name"/>
0030	<AttributeValue>
0031	<NameValue type="TextString" value="SKLC-M-3-12"/>
0032	<NameType type="Enumeration"
0033	value="UninterpretedTextString"/>
0034	</AttributeValue>
0035	</Attribute>
0036	</TemplateAttribute>
0037	</RequestPayload>
0038	</BatchItem>
0039	</RequestMessage>
0040	<ResponseMessage>
0041	<ResponseHeader>
0042	<ProtocolVersion>
0043	<ProtocolVersionMajor type="Integer" value="1"/>
0044	<ProtocolVersionMinor type="Integer" value="2"/>
0045	</ProtocolVersion>
0046	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0047	<BatchCount type="Integer" value="1"/>
0048	</ResponseHeader>
0049	<BatchItem>
0050	<Operation type="Enumeration" value="Create"/>
0051	<ResultStatus type="Enumeration" value="Success"/>
0052	<ResponsePayload>
0053	<ObjectType type="Enumeration" value="SymmetricKey"/>
0054	<UniqueIdentifier type="TextString"
0055	value="\$UNIQUE_IDENTIFIER_0"/>
0056	</ResponsePayload>
0057	</BatchItem>
0058	</ResponseMessage>
0059	# TIME 1
0060	<RequestMessage>
0061	<RequestHeader>
0062	<ProtocolVersion>
0063	<ProtocolVersionMajor type="Integer" value="1"/>
0064	<ProtocolVersionMinor type="Integer" value="2"/>
0065	</ProtocolVersion>
0066	<BatchCount type="Integer" value="1"/>
0067	</RequestHeader>
0068	<BatchItem>
0069	<Operation type="Enumeration" value="GetAttributes"/>
0070	<RequestPayload>
	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
	<AttributeName type="TextString" value="State"/>
	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
	<AttributeName type="TextString" value="Unique Identifier"/>
	<AttributeName type="TextString" value="Object Type"/>

0071	<AttributeName type="TextString" value="Cryptographic
0072	Algorithm"/>
0073	<AttributeName type="TextString" value="Cryptographic
0074	Length"/>
0075	<AttributeName type="TextString" value="Digest"/>
0076	<AttributeName type="TextString" value="Initial Date"/>
0077	<AttributeName type="TextString" value="Last Change Date"/>
0078	</RequestPayload>
0079	</BatchItem>
0080	</RequestMessage>
0081	<ResponseMessage>
0082	<ResponseHeader>
0083	<ProtocolVersion>
0084	<ProtocolVersionMajor type="Integer" value="1"/>
0085	<ProtocolVersionMinor type="Integer" value="2"/>
0086	</ProtocolVersion>
0087	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0088	<BatchCount type="Integer" value="1"/>
0089	</ResponseHeader>
0090	<BatchItem>
0091	<Operation type="Enumeration" value="GetAttributes"/>
0092	<ResultStatus type="Enumeration" value="Success"/>
0093	<ResponsePayload>
0094	<UniqueIdentifier type="TextString"
0095	value="\$UNIQUE_IDENTIFIER_0"/>
0096	<Attribute>
0097	<AttributeName type="TextString" value="State"/>
0098	<AttributeValue type="Enumeration" value="PreActive"/>
0099	</Attribute>
0100	<Attribute>
0101	<AttributeName type="TextString" value="Cryptographic Usage
0102	Mask"/>
0103	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0104	</Attribute>
0105	<Attribute>
0106	<AttributeName type="TextString" value="Unique Identifier"/>
0107	<AttributeValue type="TextString"
0108	value="\$UNIQUE_IDENTIFIER_0"/>
0109	</Attribute>
0110	<Attribute>
0111	<AttributeName type="TextString" value="Object Type"/>
0112	<AttributeValue type="Enumeration" value="SymmetricKey"/>
0113	</Attribute>
0114	<Attribute>
0115	<AttributeName type="TextString" value="Cryptographic
0116	Algorithm"/>
0117	<AttributeValue type="Enumeration" value="AES"/>
0118	</Attribute>
0119	<Attribute>
0120	<AttributeName type="TextString" value="Cryptographic
0121	Length"/>
	<AttributeValue type="Integer" value="256"/>
	</Attribute>
	<Attribute>
	<AttributeName type="TextString" value="Digest"/>
	<AttributeValue>
	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
	<DigestValue type="ByteString"

0122	value="bc12861408b8ac72cdb3b2748ad342b7dc519bd109046a1b931fdaed73591f29"/>
0123	<KeyFormatType type="Enumeration" value="Raw"/>
0124	</AttributeValue>
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>
0136	# TIME 2 <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>
0168	# TIME 3 <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>
# TIME 5	
0248	<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"
0333	value="\$UNIQUE_IDENTIFIER_0"/>
0334	</RequestPayload>
0335	</BatchItem>
0336	</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"
0350	value="\$UNIQUE_IDENTIFIER_0"/>
0351	</ResponsePayload>
0352	</BatchItem>
0352	</ResponseMessage>

134

135 3.4 Optional Test Cases KMIP 1.0

136 This section documents the test cases that a client or server conformant to the Symmetric Key Lifecycle
137 Profile MAY support under KMIP Specification 1.0.

138 3.4.1 SKLC-O-1-10

139 Create, GetAttributes, Destroy, GetAttributes

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Length"/>
0022	<AttributeValue type="Integer" value="256"/>
0023	</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-1-10"/>
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
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" value="\$UNIQUE_IDENTIFIER_0"/>
0068	<AttributeName type="TextString" value="State"/>
0069	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0070	<AttributeName type="TextString" value="Unique Identifier"/>
0071	<AttributeName type="TextString" value="Object Type"/>
0072	<AttributeName type="TextString" value="Cryptographic Algorithm"/>

0073	Length"/>
0074	<AttributeName type="TextString" value="Digest"/>
0075	<AttributeName type="TextString" value="Initial Date"/>
0076	<AttributeName type="TextString" value="Last Change Date"/>
0077	<AttributeName type="TextString" value="Activation Date"/>
0078	</RequestPayload>
0079	</BatchItem>
0080	</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"/>

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>
0136	# TIME 2 <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>
0168	# TIME 3 <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"

```

0226     value="bf60cac2a3f82e6added839c87b0bdbbc386d6280c14c8f09ca96e098365f7
0227     fe3"/>
0228     </AttributeValue>
0229     </Attribute>
0230     <Attribute>
0231         <AttributeName type="TextString" value="Initial Date"/>
0232         <AttributeValue type="DateTime" value="2013-01-
11T00:39:11+00:00"/>
0233     </Attribute>
0234     <Attribute>
0235         <AttributeName type="TextString" value="Last Change Date"/>
0236         <AttributeValue type="DateTime" value="2013-01-
11T00:39:11+00:00"/>
0237     </Attribute>
0238     <Attribute>
0239         <AttributeName type="TextString" value="Lease Time"/>
0240         <AttributeValue type="Interval" value="3600"/>
0241     </Attribute>
0242     <Attribute>
0243         <AttributeName type="TextString" value="Name"/>
0244         <AttributeValue>
0245             <NameValue type="TextString" value="SKLC-O-1-10"/>
0246             <NameType type="Enumeration"
value="UninterpretedTextString"/>
0247         </AttributeValue>
0248     </Attribute>
0249     <Attribute>
0250         <AttributeName type="TextString" value="State"/>
0251         <AttributeValue type="Enumeration" value="Destroyed"/>
0252     </Attribute>
0253 </ResponsePayload>
</BatchItem>
</ResponseMessage>

```

140

141

142 3.5 Optional Test Cases KMIP 1.1

143 This section documents the test cases that a client or server conformant to the Symmetric Key Lifecycle
144 Profile SHALL support under KMIP Specification 1.1.

145 3.5.1 SKLC-O-1-11

146 Create, GetAttributes, Destroy, GetAttributes

```

0001 # TIME 0
0002 <RequestMessage>
0003     <RequestHeader>
0004         <ProtocolVersion>
0005             <ProtocolVersionMajor type="Integer" value="1"/>
0006             <ProtocolVersionMinor type="Integer" value="1"/>
0007         </ProtocolVersion>
0008         <BatchCount type="Integer" value="1"/>
0009     </RequestHeader>
0010     <BatchItem>
0011         <Operation type="Enumeration" value="Create"/>
0012         <RequestPayload>
0013             <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>
0055	# TIME 1
0056	<RequestMessage>
0057	<RequestHeader>
0058	<ProtocolVersion>
0059	<ProtocolVersionMajor type="Integer" value="1"/>
0060	<ProtocolVersionMinor type="Integer" value="1"/>
0061	</ProtocolVersion>
0062	<BatchCount type="Integer" value="1"/>
0063	</RequestHeader>
0064	<BatchItem>
0065	<Operation type="Enumeration" value="GetAttributes"/>

0065	<RequestPayload>
0066	<UniqueIdentifier type="TextString"
0067	value="\$UNIQUE_IDENTIFIER_0"/>
0068	<AttributeName type="TextString" value="State"/>
0069	<AttributeName type="TextString" value="Cryptographic Usage
0070	Mask"/>
0071	<AttributeName type="TextString" value="Unique Identifier"/>
0072	<AttributeName type="TextString" value="Object Type"/>
0073	<AttributeName type="TextString" value="Cryptographic
0074	Algorithm"/>
0075	<AttributeName type="TextString" value="Cryptographic
0076	Length"/>
0077	<AttributeName type="TextString" value="Digest"/>
0078	<AttributeName type="TextString" value="Initial Date"/>
0079	<AttributeName type="TextString" value="Last Change Date"/>
0080	<AttributeName type="TextString" value="Activation Date"/>
0081	</RequestPayload>
0082	</BatchItem>
0083	</RequestMessage>
0084	<ResponseMessage>
0085	<ResponseHeader>
0086	<ProtocolVersion>
0087	<ProtocolVersionMajor type="Integer" value="1"/>
0088	<ProtocolVersionMinor type="Integer" value="1"/>
0089	</ProtocolVersion>
0090	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0091	<BatchCount type="Integer" value="1"/>
0092	</ResponseHeader>
0093	<BatchItem>
0094	<Operation type="Enumeration" value="GetAttributes"/>
0095	<ResultStatus type="Enumeration" value="Success"/>
0096	<ResponsePayload>
0097	<UniqueIdentifier type="TextString"
0098	value="\$UNIQUE_IDENTIFIER_0"/>
0099	<Attribute>
0100	<AttributeName type="TextString" value="State"/>
0101	<AttributeValue type="Enumeration" value="PreActive"/>
0102	</Attribute>
0103	<Attribute>
0104	<AttributeName type="TextString" value="Cryptographic Usage
0105	Mask"/>
0106	<AttributeValue type="Integer" value="Decrypt Encrypt"/>
0107	</Attribute>
0108	<Attribute>
0109	<AttributeName type="TextString" value="Unique Identifier"/>
0110	<AttributeValue type="TextString"
0111	value="\$UNIQUE_IDENTIFIER_0"/>
0112	</Attribute>
0113	<Attribute>
0114	<AttributeName type="TextString" value="Object Type"/>
	<AttributeValue type="Enumeration" value="SymmetricKey"/>
	</Attribute>
	<Attribute>
	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
	<AttributeValue type="Enumeration" value="AES"/>
	</Attribute>
	<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"

0166	value="\$UNIQUE_IDENTIFIER_0"/>
0167	</ResponsePayload>
0168	</BatchItem>
0168	</ResponseMessage>
0169	# 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	</RequestPayload>
0183	</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"
0198	value="\$UNIQUE_IDENTIFIER_0"/>
0198	<Attribute>
0199	<AttributeName type="TextString" value="Unique Identifier"/>
0200	<AttributeValue type="TextString"
0201	value="\$UNIQUE_IDENTIFIER_0"/>
0202	</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
0208	Algorithm"/>
0208	<AttributeValue type="Enumeration" value="AES"/>
0209	</Attribute>
0210	<Attribute>
0211	<AttributeName type="TextString" value="Cryptographic
0212	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-1-11"/>
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>

```

147

148

149 3.6 Optional Test Cases KMIP 1.2

150 This section documents the test cases that a client or server conformant to the Symmetric Key Lifecycle
151 Profile MAY support under KMIP Specification 1.2.

152 3.6.1 SKLC-O-1-12

153 Create, GetAttributes, Destroy, GetAttributes

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Create"/>
0011	<RequestPayload>
0012	<ObjectType type="Enumeration" value="SymmetricKey"/>
0013	<TemplateAttribute>
0014	<Attribute>
0015	<AttributeName type="TextString" value="Cryptographic
0016	Algorithm"/>
0017	<AttributeValue type="Enumeration" value="AES"/>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Cryptographic
0021	Length"/>
0022	<AttributeValue type="Integer" value="256"/>
0023	</Attribute>
0024	<Attribute>
0025	<AttributeName type="TextString" value="Cryptographic
0026	Usage Mask"/>
0027	<AttributeValue type="Integer" value="Encrypt Decrypt"/>
0028	</Attribute>
0029	<Attribute>
0030	<AttributeName type="TextString" value="Name"/>
0031	<AttributeValue>
0032	<NameValue type="TextString" value="SKLC-O-1-12"/>
0033	<NameType type="Enumeration"
0034	value="UninterpretedTextString"/>
0035	</AttributeValue>
0036	</Attribute>
0037	</TemplateAttribute>
0038	</RequestPayload>
0039	</BatchItem>
0040	</RequestMessage>
0041	<ResponseMessage>
0042	<ResponseHeader>
0043	<ProtocolVersion>
0044	<ProtocolVersionMajor type="Integer" value="1"/>
0045	<ProtocolVersionMinor type="Integer" value="2"/>
0046	</ProtocolVersion>
0047	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0048	<BatchCount type="Integer" value="1"/>
0049	</ResponseHeader>
0050	<BatchItem>
	<Operation type="Enumeration" value="Create"/>
	<ResultStatus type="Enumeration" value="Success"/>
	<ResponsePayload>
	<ObjectType type="Enumeration" value="SymmetricKey"/>

0051	<UniqueIdentifier type="TextString"
0052	value="\$UNIQUE_IDENTIFIER_0"/>
0053	</ResponsePayload>
0054	</BatchItem>
	</ResponseMessage>
	# TIME 1
0055	<RequestMessage>
0056	<RequestHeader>
0057	<ProtocolVersion>
0058	<ProtocolVersionMajor type="Integer" value="1"/>
0059	<ProtocolVersionMinor type="Integer" value="2"/>
0060	</ProtocolVersion>
0061	<BatchCount type="Integer" value="1"/>
0062	</RequestHeader>
0063	<BatchItem>
0064	<Operation type="Enumeration" value="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>
	# TIME 2
0137	<RequestMessage>
0138	<RequestHeader>
0139	<ProtocolVersion>
0140	<ProtocolVersionMajor type="Integer" value="1"/>
0141	<ProtocolVersionMinor type="Integer" value="2"/>
0142	</ProtocolVersion>
0143	<BatchCount type="Integer" value="1"/>
0144	</RequestHeader>
0145	<BatchItem>
0146	<Operation type="Enumeration" value="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	</BatchItem>

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-1-12"/>
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>

154

155

156

4 Symmetric Key Lifecycle Profile - Test Cases

This section documents the test cases for a KMIP server performing symmetric key lifecycle operations based on requests received from a KMIP client.

Note: the values for the returned items and the custom attributes are illustrative. Actual values from a real client system will vary.

4.1 Mandatory Test Cases

This section documents the test cases that a client or server conformant to the Symmetric Key Lifecycle Profile SHALL support.

5 Conformance

5.1 Conformance Statement

KMIP client and server implementations conformant to this profile:

1. SHALL support the Authentication Suite conditions (2.1) and;
2. SHALL support the Baseline conditions (2.2) and;
3. SHALL support all Mandatory Test Cases (3.1 and 3.2 and 3.3), for each supported protocol version (major and minor), returning results in accordance with the test cases.

5.2 Permitted Test Case Variations

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

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

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

5.2.1 Variable Items

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

1. UniqueIdentifier
2. PrivateKeyUniqueIdentifier
3. PublicKeyUniqueIdentifier
4. UniqueBatchItemIdentifier
5. AsynchronousCorrelationValue
6. TimeStamp
7. KeyValue / KeyMaterial including:
 - a. key material content returned for managed cryptographic objects which are generated by the server
 - b. wrapped versions of keys where the wrapping key is dynamic or the wrapping contains variable output for each wrap operation
8. For response containing the output of cryptographic operation in Data / SignatureData/ MACData / IVCounterNonce where:
 - a. the managed object is generated by the server; or
 - b. the operation inherently contains variable output
9. For the following DateTime attributes where the value is not specified in the request as a fixed DateTime value:
 - a. ActivationDate
 - b. ArchiveDate
 - c. CompromiseDate
 - d. CompromiseOccurrenceDate
 - e. DeactivationDate
 - f. DestroyDate

- 205 g. InitialDate
- 206 h. LastChangeDate
- 207 i. ProtectStartDate
- 208 j. ProcessStopDate
- 209 k. ValidityDate
- 210 l. OriginalCreationDate
- 211 10. LinkedObjectIdentifier
- 212 11. DigestValue
 - 213 a. For those managed cryptographic objects which are dynamically generated
- 214 12. KeyFormatType
 - 215 a. The key format type selected by the server when it creates managed objects
- 216 13. Digest
 - 217 a. The HashingAlgorithm selected by the server when it calculates the digest for a managed
 - 218 object for which it has access to the key material
 - 219 b. The Digest Value
- 220 14. Extensions reported in Query for ExtensionList and ExtensionMap
- 221 15. Application Namespaces reported in Query
- 222 16. Object Types reported in Query other than those noted as required in this profile
- 223 17. Operation Types reported in Query other than those noted as required in this profile (or any
- 224 referenced profile documents)
- 225 18. For TextString attribute values containing test identifiers:
 - 226 a. Additional vendor or application prefixes
- 227 19. Additional attributes beyond those noted in the response
- 228

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

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

245 5.2.2 Variable behavior

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

- 247
248
249
250
251
252
253
254
255
1. A test may omit the clean-up requests and responses (containing Revoke and/or Destroy) at the end of the test provided there is a separate mechanism to remove the created objects during testing.
 2. A test may omit the test identifiers if the client is unable to include them in requests. This includes the following attributes:
 - a. Name; and
 - b. x-ID

Appendix A. Acknowledgments

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

Participants:

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

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

363 Michael Yoder, Vormetric. Inc.
364 Magda Zdunkiewicz, Cryptsoft
365 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.

Appendix C. Revision History

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.