

# KMIP Asymmetric Key Lifecycle Profile Version 1.0

## Committee Specification Draft 02 / Public Review Draft 02

19 June 2014

### Specification URIs

#### This version:

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

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

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

#### Previous version:

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

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

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

#### Latest version:

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

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

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

#### Technical Committee:

OASIS Key Management Interoperability Protocol (KMIP) TC

#### Chairs:

Subhash Sankuratripati ([Subhash.Sankuratripati@netapp.com](mailto:Subhash.Sankuratripati@netapp.com)), NetApp

Saikat Saha ([saiikat.saha@oracle.com](mailto:saiikat.saha@oracle.com)), Oracle

#### Editors:

Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)), Cryptsoft Pty Ltd.

Robert Lockhart ([Robert.Lockhart@thalesesec.com](mailto:Robert.Lockhart@thalesesec.com)), Thales e-Security

#### Related work:

This specification is related to:

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

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

**Abstract:**

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

**Status:**

This document was last revised or approved by the OASIS Key Management Interoperability Protocol (KMIP) TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document.

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

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

**Citation format:**

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

**[kmip-asym-key-v1.0]**

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

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

---

## Notices

Copyright © OASIS Open 2014. All Rights Reserved.

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

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

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

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

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

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

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

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

---

# Table of Contents

1	Introduction.....	5
1.1	Terminology.....	5
1.2	Normative References.....	5
2	Asymmetric Key Lifecycle Profile.....	6
2.1	Authentication Suite.....	6
2.2	Asymmetric Key Lifecycle - Client.....	6
2.3	Asymmetric Key Lifecycle - Server.....	6
3	Asymmetric Key Lifecycle Profile - Test Cases.....	8
3.1	Mandatory Test Cases KMIP v1.0.....	8
3.1.1	AKLC-M-1-10.....	8
3.1.2	AKLC-M-2-10.....	14
3.1.3	AKLC-M-3-10.....	22
3.2	Mandatory Test Cases KMIP v1.1.....	31
3.2.1	AKLC-M-1-11.....	31
3.2.2	AKLC-M-2-11.....	37
3.2.3	AKLC-M-3-11.....	45
3.3	Mandatory Test Cases KMIP v1.2.....	54
3.3.1	AKLC-M-1-12.....	54
3.3.2	AKLC-M-2-12.....	60
3.3.3	AKLC-M-3-12.....	69
3.4	Optional Test Cases KMIP v1.0.....	77
3.4.1	AKLC-O-1-10.....	77
3.5	Optional Test Cases KMIP v1.1.....	87
3.5.1	AKLC-O-1-11.....	87
3.6	Optional Test Cases KMIP v1.2.....	97
3.6.1	AKLC-O-1-12.....	97
4	Conformance.....	108
4.1	Asymmetric Key Lifecycle Client KMIP v1.0 Profile Conformance.....	108
4.2	Asymmetric Key Lifecycle Client KMIP v1.1 Profile Conformance.....	108
4.3	Asymmetric Key Lifecycle Client KMIP v1.2 Profile Conformance.....	108
4.4	Asymmetric Key Lifecycle Client KMIP v1.0 Profile Conformance.....	108
4.5	Asymmetric Key Lifecycle Client KMIP v1.1 Profile Conformance.....	108
4.6	Asymmetric Key Lifecycle Client KMIP v1.2 Profile Conformance.....	108
4.7	Permitted Test Case Variations.....	109
4.7.1	Variable Items.....	109
4.7.2	Variable behavior.....	110
Appendix A.	Acknowledgments.....	111
Appendix B.	KMIP Specification Cross Reference.....	114
Appendix C.	Revision History.....	119

---

# 1 Introduction

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

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

## 1.1 Terminology

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

## 1.2 Normative References

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

---

## 36 2 Asymmetric Key Lifecycle Profile

37 The Asymmetric Key Lifecycle Profile is a KMIP server performing asymmetric key lifecycle operations  
38 based on requests received from a KMIP client.

### 39 2.1 Authentication Suite

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

### 43 2.2 Asymmetric Key Lifecycle - Client

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

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

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

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

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

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

50 KMIP clients conformant to this profile:

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

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

### 55 2.3 Asymmetric Key Lifecycle - Server

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

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

58 KMIP servers conformant to this profile under [KMIP-SPEC-1\_1]:

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

60 KMIP servers conformant to this profile under [KMIP-SPEC-1\_2]:

61 3. SHALL conform to the *Baseline Servers* of [KMIP-PROF-1\_2]

62 KMIP servers conformant to this profile:

63 4. SHALL support the following *Objects* [KMIP-SPEC]

64 a. *Public Key* [KMIP-SPEC]

65 b. *Private Key* [KMIP-SPEC]

66 c. *Key Format Type* [KMIP-SPEC]

67 5. SHALL support the following *Attributes* [KMIP-SPEC]

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

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

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

71 d. *Process Stop Date* [KMIP-SPEC]

72 6. SHALL support the following *Message Encoding* [KMIP-SPEC]:

73 a. *Cryptographic Algorithm* [KMIP-SPEC] with values:

- 74                   i. RSA
- 75           b. *Object Type* [KMIP-SPEC] with value:
- 76                   i. Public Key
- 77                   ii. Private Key
- 78           c. *Key Format Type* [KMIP-SPEC] with value:
- 79                   i. PKCS#1
- 80                   ii. PKCS#8
- 81                   iii. Transparent RSA Public Key
- 82                   iv. Transparent RSA Private Key
- 83   7. MAY support any clause within [KMIP-SPEC] provided it does not conflict with any other clause
- 84    within this section 2.3
- 85   8. MAY support extensions outside the scope of this standard (e.g., vendor extensions,
- 86    conformance clauses) that do not contradict any KMIP requirements.

## 87 3 Asymmetric Key Lifecycle Profile - Test Cases

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

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

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

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

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

### 101 3.1 Mandatory Test Cases KMIP v1.0

#### 102 3.1.1 AKLC-M-1-10

103 CreateKeyPair, GetAttributes, GetAttributes, Destroy

```
0001 # TIME 0
0002 <RequestMessage>
0003   <RequestHeader>
0004     <ProtocolVersion>
0005       <ProtocolVersionMajor type="Integer" value="1"/>
0006       <ProtocolVersionMinor type="Integer" value="0"/>
0007     </ProtocolVersion>
0008     <BatchCount type="Integer" value="1"/>
0009   </RequestHeader>
0010   <BatchItem>
0011     <Operation type="Enumeration" value="CreateKeyPair"/>
0012     <RequestPayload>
0013       <CommonTemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0016           <AttributeValue type="Enumeration" value="RSA"/>
0017         </Attribute>
0018         <Attribute>
0019           <AttributeName type="TextString" value="Cryptographic
Length"/>
0020           <AttributeValue type="Integer" value="2048"/>
0021         </Attribute>
0022         <PrivateKeyTemplateAttribute>
0023           <Attribute>
0024             <AttributeName type="TextString" value="Name"/>
0025             <AttributeValue>
0026               <NameValue type="TextString" value="AKLC-M-1-10-
private"/>
0027             <NameType type="Enumeration"
value="UninterpretedTextString"/>
```



0028	</AttributeValue>
0029	</Attribute>
0030	<Attribute>
0031	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0032	<AttributeValue type="Integer" value="Sign"/>
0033	</Attribute>
0034	</PrivateKeyTemplateAttribute>
0035	<PublicKeyTemplateAttribute>
0036	<Attribute>
0037	<AttributeName type="TextString" value="Name"/>
0038	<AttributeValue>
0039	<NameValue type="TextString" value="AKLC-M-1-10- public"/>
0040	<NameType type="Enumeration" value="UninterpretedTextString"/>
0041	</AttributeValue>
0042	</Attribute>
0043	<Attribute>
0044	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0045	<AttributeValue type="Integer" value="Verify"/>
0046	</Attribute>
0047	</PublicKeyTemplateAttribute>
0048	</RequestPayload>
0049	</BatchItem>
0050	</RequestMessage>
0051	<ResponseMessage>
0052	<ResponseHeader>
0053	<ProtocolVersion>
0054	<ProtocolVersionMajor type="Integer" value="1"/>
0055	<ProtocolVersionMinor type="Integer" value="0"/>
0056	</ProtocolVersion>
0057	<TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/>
0058	<BatchCount type="Integer" value="1"/>
0059	</ResponseHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="CreateKeyPair"/>
0062	<ResultStatus type="Enumeration" value="Success"/>
0063	<ResponsePayload>
0064	<PrivateKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0065	<PublicKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
0069	# TIME 1 <RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="0"/>
0074	</ProtocolVersion>
0075	<BatchCount type="Integer" value="1"/>
0076	</RequestHeader>
0077	<BatchItem>
0078	<Operation type="Enumeration" value="GetAttributes"/>

0079	<RequestPayload>
0080	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0081	<AttributeName type="TextString" value="State"/>
0082	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0083	<AttributeName type="TextString" value="Unique Identifier"/>
0084	<AttributeName type="TextString" value="Object Type"/>
0085	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0086	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0087	<AttributeName type="TextString" value="Digest"/>
0088	<AttributeName type="TextString" value="Initial Date"/>
0089	<AttributeName type="TextString" value="Last Change Date"/>
0090	<AttributeName type="TextString" value="Activation Date"/>
0091	</RequestPayload>
0092	</BatchItem>
0093	</RequestMessage>
0094	<ResponseMessage>
0095	<ResponseHeader>
0096	<ProtocolVersion>
0097	<ProtocolVersionMajor type="Integer" value="1"/>
0098	<ProtocolVersionMinor type="Integer" value="0"/>
0099	</ProtocolVersion>
0100	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0101	<BatchCount type="Integer" value="1"/>
0102	</ResponseHeader>
0103	<BatchItem>
0104	<Operation type="Enumeration" value="GetAttributes"/>
0105	<ResultStatus type="Enumeration" value="Success"/>
0106	<ResponsePayload>
0107	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0108	<Attribute>
0109	<AttributeName type="TextString" value="State"/>
0110	<AttributeValue type="Enumeration" value="PreActive"/>
0111	</Attribute>
0112	<Attribute>
0113	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0114	<AttributeValue type="Integer" value="Sign"/>
0115	</Attribute>
0116	<Attribute>
0117	<AttributeName type="TextString" value="Unique Identifier"/>
0118	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0119	</Attribute>
0120	<Attribute>
0121	<AttributeName type="TextString" value="Object Type"/>
0122	<AttributeValue type="Enumeration" value="PrivateKey"/>
0123	</Attribute>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0126	<AttributeValue type="Enumeration" value="RSA"/>
0127	</Attribute>
0128	</Attribute>

0129	<AttributeName type="TextString" value="Cryptographic Length"/>
0130	<AttributeValue type="Integer" value="2048"/>
0131	</Attribute>
0132	<Attribute>
0133	<AttributeName type="TextString" value="Digest"/>
0134	<AttributeValue>
0135	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0136	<DigestValue type="ByteString" value="8eb422ae2b006a05d3c8a542a28536735241b6dc1c37926bc8007bd6220d9230"/>
0137	</AttributeValue>
0138	</Attribute>
0139	<Attribute>
0140	<AttributeName type="TextString" value="Initial Date"/>
0141	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0142	</Attribute>
0143	<Attribute>
0144	<AttributeName type="TextString" value="Last Change Date"/>
0145	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0146	</Attribute>
0147	</ResponsePayload>
0148	</BatchItem>
0149	</ResponseMessage>
	# TIME 2
0150	<RequestMessage>
0151	<RequestHeader>
0152	<ProtocolVersion>
0153	<ProtocolVersionMajor type="Integer" value="1"/>
0154	<ProtocolVersionMinor type="Integer" value="0"/>
0155	</ProtocolVersion>
0156	<BatchCount type="Integer" value="1"/>
0157	</RequestHeader>
0158	<BatchItem>
0159	<Operation type="Enumeration" value="GetAttributes"/>
0160	<RequestPayload>
0161	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0162	<AttributeName type="TextString" value="State"/>
0163	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0164	<AttributeName type="TextString" value="Unique Identifier"/>
0165	<AttributeName type="TextString" value="Object Type"/>
0166	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0167	<AttributeName type="TextString" value="Cryptographic Length"/>
0168	<AttributeName type="TextString" value="Digest"/>
0169	<AttributeName type="TextString" value="Initial Date"/>
0170	<AttributeName type="TextString" value="Last Change Date"/>
0171	<AttributeName type="TextString" value="Activation Date"/>
0172	</RequestPayload>
0173	</BatchItem>
0174	</RequestMessage>
0175	<ResponseMessage>
0176	<ResponseHeader>

```

0177     <ProtocolVersion>
0178         <ProtocolVersionMajor type="Integer" value="1"/>
0179         <ProtocolVersionMinor type="Integer" value="0"/>
0180     </ProtocolVersion>
0181     <TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0182     <BatchCount type="Integer" value="1"/>
0183 </ResponseHeader>
0184 <BatchItem>
0185     <Operation type="Enumeration" value="GetAttributes"/>
0186     <ResultStatus type="Enumeration" value="Success"/>
0187     <ResponsePayload>
0188         <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0189     <Attribute>
0190         <AttributeName type="TextString" value="State"/>
0191         <AttributeValue type="Enumeration" value="PreActive"/>
0192     </Attribute>
0193     <Attribute>
0194         <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0195         <AttributeValue type="Integer" value="Verify"/>
0196     </Attribute>
0197     <Attribute>
0198         <AttributeName type="TextString" value="Unique Identifier"/>
0199         <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0200     </Attribute>
0201     <Attribute>
0202         <AttributeName type="TextString" value="Object Type"/>
0203         <AttributeValue type="Enumeration" value="PublicKey"/>
0204     </Attribute>
0205     <Attribute>
0206         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0207         <AttributeValue type="Enumeration" value="RSA"/>
0208     </Attribute>
0209     <Attribute>
0210         <AttributeName type="TextString" value="Cryptographic
Length"/>
0211         <AttributeValue type="Integer" value="2048"/>
0212     </Attribute>
0213     <Attribute>
0214         <AttributeName type="TextString" value="Digest"/>
0215         <AttributeValue>
0216             <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0217             <DigestValue type="ByteString"
value="82bcff8afab753809db804e654013ded708c3996a50c6ce9313f9b3915442
ce9"/>
0218         </AttributeValue>
0219     </Attribute>
0220     <Attribute>
0221         <AttributeName type="TextString" value="Initial Date"/>
0222         <AttributeValue type="DateTime" value="2013-01-
11T08:19:49+00:00"/>
0223     </Attribute>
0224     <Attribute>
0225         <AttributeName type="TextString" value="Last Change Date"/>
0226         <AttributeValue type="DateTime" value="2013-01-

```

0227	11T08:19:49+00:00"/>
0228	</Attribute>
0229	</ResponsePayload>
0230	</BatchItem>
0231	</ResponseMessage>
0231	# TIME 3
0232	<RequestMessage>
0233	<RequestHeader>
0234	<ProtocolVersion>
0235	<ProtocolVersionMajor type="Integer" value="1"/>
0236	<ProtocolVersionMinor type="Integer" value="0"/>
0237	</ProtocolVersion>
0238	<BatchCount type="Integer" value="1"/>
0239	</RequestHeader>
0240	<BatchItem>
0241	<Operation type="Enumeration" value="Destroy"/>
0242	<RequestPayload>
0243	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0244	</RequestPayload>
0245	</BatchItem>
0246	</RequestMessage>
0247	<ResponseMessage>
0248	<ResponseHeader>
0249	<ProtocolVersion>
0250	<ProtocolVersionMajor type="Integer" value="1"/>
0251	<ProtocolVersionMinor type="Integer" value="0"/>
0252	</ProtocolVersion>
0253	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0254	<BatchCount type="Integer" value="1"/>
0255	</ResponseHeader>
0256	<BatchItem>
0257	<Operation type="Enumeration" value="Destroy"/>
0258	<ResultStatus type="Enumeration" value="Success"/>
0259	<ResponsePayload>
0260	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0261	</ResponsePayload>
0262	</BatchItem>
0263	</ResponseMessage>
0263	# TIME 4
0264	<RequestMessage>
0265	<RequestHeader>
0266	<ProtocolVersion>
0267	<ProtocolVersionMajor type="Integer" value="1"/>
0268	<ProtocolVersionMinor type="Integer" value="0"/>
0269	</ProtocolVersion>
0270	<BatchCount type="Integer" value="1"/>
0271	</RequestHeader>
0272	<BatchItem>
0273	<Operation type="Enumeration" value="Destroy"/>
0274	<RequestPayload>
0275	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0276	</RequestPayload>
0277	</BatchItem>
0278	</RequestMessage>
0278	<ResponseMessage>

```

0279 <ResponseHeader>
0280 <ProtocolVersion>
0281 <ProtocolVersionMajor type="Integer" value="1"/>
0282 <ProtocolVersionMinor type="Integer" value="0"/>
0283 </ProtocolVersion>
0284 <TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0285 <BatchCount type="Integer" value="1"/>
0286 </ResponseHeader>
0287 <BatchItem>
0288 <Operation type="Enumeration" value="Destroy"/>
0289 <ResultStatus type="Enumeration" value="Success"/>
0290 <ResponsePayload>
0291 <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0292 </ResponsePayload>
0293 </BatchItem>
0294 </ResponseMessage>

```

104

### 105 3.1.2 AKLC-M-2-10

106 CreateKeyPair, 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="CreateKeyPair"/>
0011 <RequestPayload>
0012 <CommonTemplateAttribute>
0013 <Attribute>
0014 <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0015 <AttributeValue type="Enumeration" value="RSA"/>
0016 </Attribute>
0017 <Attribute>
0018 <AttributeName type="TextString" value="Cryptographic
Length"/>
0019 <AttributeValue type="Integer" value="2048"/>
0020 </Attribute>
0021 </CommonTemplateAttribute>
0022 <PrivateKeyTemplateAttribute>
0023 <Attribute>
0024 <AttributeName type="TextString" value="Name"/>
0025 <AttributeValue>
0026 <NameValue type="TextString" value="AKLC-M-2-10-
private"/>
0027 <NameType type="Enumeration"
value="UninterpretedTextString"/>
0028 </AttributeValue>
0029 </Attribute>
0030 </Attribute>

```

0031	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0032	<AttributeValue type="Integer" value="Sign"/>
0033	</Attribute>
0034	</PrivateKeyTemplateAttribute>
0035	<PublicKeyTemplateAttribute>
0036	<Attribute>
0037	<AttributeName type="TextString" value="Name"/>
0038	<AttributeValue>
0039	<NameValue type="TextString" value="AKLC-M-2-10-public"/>
0040	<NameType type="Enumeration" value="UninterpretedTextString"/>
0041	</AttributeValue>
0042	</Attribute>
0043	<Attribute>
0044	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0045	<AttributeValue type="Integer" value="Verify"/>
0046	</Attribute>
0047	</PublicKeyTemplateAttribute>
0048	</RequestPayload>
0049	</BatchItem>
0050	</RequestMessage>
0051	<ResponseMessage>
0052	<ResponseHeader>
0053	<ProtocolVersion>
0054	<ProtocolVersionMajor type="Integer" value="1"/>
0055	<ProtocolVersionMinor type="Integer" value="0"/>
0056	</ProtocolVersion>
0057	<TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/>
0058	<BatchCount type="Integer" value="1"/>
0059	</ResponseHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="CreateKeyPair"/>
0062	<ResultStatus type="Enumeration" value="Success"/>
0063	<ResponsePayload>
0064	<PrivateKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0065	<PublicKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
0069	# TIME 1 <RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="0"/>
0074	</ProtocolVersion>
0075	<BatchCount type="Integer" value="1"/>
0076	</RequestHeader>
0077	<BatchItem>
0078	<Operation type="Enumeration" value="GetAttributes"/>
0079	<RequestPayload>
0080	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>

```

0081     <AttributeName type="TextString" value="State"/>
0082     <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0083     <AttributeName type="TextString" value="Unique Identifier"/>
0084     <AttributeName type="TextString" value="Object Type"/>
0085     <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0086     <AttributeName type="TextString" value="Cryptographic
Length"/>
0087     <AttributeName type="TextString" value="Digest"/>
0088     <AttributeName type="TextString" value="Initial Date"/>
0089     <AttributeName type="TextString" value="Last Change Date"/>
0090     </RequestPayload>
0091   </BatchItem>
0092 </RequestMessage>

0093 <ResponseMessage>
0094   <ResponseHeader>
0095     <ProtocolVersion>
0096       <ProtocolVersionMajor type="Integer" value="1"/>
0097       <ProtocolVersionMinor type="Integer" value="0"/>
0098     </ProtocolVersion>
0099     <TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0100     <BatchCount type="Integer" value="1"/>
0101   </ResponseHeader>
0102   <BatchItem>
0103     <Operation type="Enumeration" value="GetAttributes"/>
0104     <ResultStatus type="Enumeration" value="Success"/>
0105     <ResponsePayload>
0106       <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0107       <Attribute>
0108         <AttributeName type="TextString" value="State"/>
0109         <AttributeValue type="Enumeration" value="PreActive"/>
0110       </Attribute>
0111       <Attribute>
0112         <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0113         <AttributeValue type="Integer" value="Sign"/>
0114       </Attribute>
0115       <Attribute>
0116         <AttributeName type="TextString" value="Unique Identifier"/>
0117         <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0118       </Attribute>
0119       <Attribute>
0120         <AttributeName type="TextString" value="Object Type"/>
0121         <AttributeValue type="Enumeration" value="PrivateKey"/>
0122       </Attribute>
0123       <Attribute>
0124         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0125         <AttributeValue type="Enumeration" value="RSA"/>
0126       </Attribute>
0127       <Attribute>
0128         <AttributeName type="TextString" value="Cryptographic
Length"/>
0129         <AttributeValue type="Integer" value="2048"/>
0130       </Attribute>

```



0131	<Attribute>
0132	<AttributeName type="TextString" value="Digest"/>
0133	<AttributeValue>
0134	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0135	<DigestValue type="ByteString"
	value="8eb422ae2b006a05d3c8a542a28536735241b6dc1c37926bc8007bd6220d9
	230"/>
0136	</AttributeValue>
0137	</Attribute>
0138	<Attribute>
0139	<AttributeName type="TextString" value="Initial Date"/>
0140	<AttributeValue type="DateTime" value="2013-01-
	11T08:18:21+00:00"/>
0141	</Attribute>
0142	<Attribute>
0143	<AttributeName type="TextString" value="Last Change Date"/>
0144	<AttributeValue type="DateTime" value="2013-01-
	11T08:18:21+00:00"/>
0145	</Attribute>
0146	</ResponsePayload>
0147	</BatchItem>
0148	</ResponseMessage>
	# TIME 2
0149	<RequestMessage>
0150	<RequestHeader>
0151	<ProtocolVersion>
0152	<ProtocolVersionMajor type="Integer" value="1"/>
0153	<ProtocolVersionMinor type="Integer" value="0"/>
0154	</ProtocolVersion>
0155	<BatchCount type="Integer" value="1"/>
0156	</RequestHeader>
0157	<BatchItem>
0158	<Operation type="Enumeration" value="Activate"/>
0159	<RequestPayload>
0160	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0161	</RequestPayload>
0162	</BatchItem>
0163	</RequestMessage>
0164	<ResponseMessage>
0165	<ResponseHeader>
0166	<ProtocolVersion>
0167	<ProtocolVersionMajor type="Integer" value="1"/>
0168	<ProtocolVersionMinor type="Integer" value="0"/>
0169	</ProtocolVersion>
0170	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0171	<BatchCount type="Integer" value="1"/>
0172	</ResponseHeader>
0173	<BatchItem>
0174	<Operation type="Enumeration" value="Activate"/>
0175	<ResultStatus type="Enumeration" value="Success"/>
0176	<ResponsePayload>
0177	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0178	</ResponsePayload>
0179	</BatchItem>
0180	</ResponseMessage>
	# TIME 3

```

0181 <RequestMessage>
0182   <RequestHeader>
0183     <ProtocolVersion>
0184       <ProtocolVersionMajor type="Integer" value="1"/>
0185       <ProtocolVersionMinor type="Integer" value="0"/>
0186     </ProtocolVersion>
0187     <BatchCount type="Integer" value="1"/>
0188   </RequestHeader>
0189   <BatchItem>
0190     <Operation type="Enumeration" value="GetAttributes"/>
0191     <RequestPayload>
0192       <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0193       <AttributeName type="TextString" value="State"/>
0194       <AttributeName type="TextString" value="Activation Date"/>
0195       <AttributeName type="TextString" value="Deactivation Date"/>
0196     </RequestPayload>
0197   </BatchItem>
0198 </RequestMessage>
0199 <ResponseMessage>
0200   <ResponseHeader>
0201     <ProtocolVersion>
0202       <ProtocolVersionMajor type="Integer" value="1"/>
0203       <ProtocolVersionMinor type="Integer" value="0"/>
0204     </ProtocolVersion>
0205     <TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0206     <BatchCount type="Integer" value="1"/>
0207   </ResponseHeader>
0208   <BatchItem>
0209     <Operation type="Enumeration" value="GetAttributes"/>
0210     <ResultStatus type="Enumeration" value="Success"/>
0211     <ResponsePayload>
0212       <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0213       <Attribute>
0214         <AttributeName type="TextString" value="State"/>
0215         <AttributeValue type="Enumeration" value="Active"/>
0216       </Attribute>
0217       <Attribute>
0218         <AttributeName type="TextString" value="Activation Date"/>
0219         <AttributeValue type="DateTime" value="2013-01-
10T23:36:01+00:00"/>
0220       </Attribute>
0221     </ResponsePayload>
0222   </BatchItem>
0223 </ResponseMessage>
# TIME 4
0224 <RequestMessage>
0225   <RequestHeader>
0226     <ProtocolVersion>
0227       <ProtocolVersionMajor type="Integer" value="1"/>
0228       <ProtocolVersionMinor type="Integer" value="0"/>
0229     </ProtocolVersion>
0230     <BatchCount type="Integer" value="1"/>
0231   </RequestHeader>
0232   <BatchItem>
0233     <Operation type="Enumeration" value="GetAttributes"/>
0234     <RequestPayload>

```

0235	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0236	<AttributeName type="TextString" value="State"/>
0237	<AttributeName type="TextString" value="Activation Date"/>
0238	<AttributeName type="TextString" value="Deactivation Date"/>
0239	</RequestPayload>
0240	</BatchItem>
0241	</RequestMessage>
0242	<ResponseMessage>
0243	<ResponseHeader>
0244	<ProtocolVersion>
0245	<ProtocolVersionMajor type="Integer" value="1"/>
0246	<ProtocolVersionMinor type="Integer" value="0"/>
0247	</ProtocolVersion>
0248	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0249	<BatchCount type="Integer" value="1"/>
0250	</ResponseHeader>
0251	<BatchItem>
0252	<Operation type="Enumeration" value="GetAttributes"/>
0253	<ResultStatus type="Enumeration" value="Success"/>
0254	<ResponsePayload>
0255	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0256	<Attribute>
0257	<AttributeName type="TextString" value="State"/>
0258	<AttributeValue type="Enumeration" value="PreActive"/>
0259	</Attribute>
0260	</ResponsePayload>
0261	</BatchItem>
0262	</ResponseMessage>
0263	# TIME 5 <RequestMessage>
0264	<RequestHeader>
0265	<ProtocolVersion>
0266	<ProtocolVersionMajor type="Integer" value="1"/>
0267	<ProtocolVersionMinor type="Integer" value="0"/>
0268	</ProtocolVersion>
0269	<BatchCount type="Integer" value="1"/>
0270	</RequestHeader>
0271	<BatchItem>
0272	<Operation type="Enumeration" value="Destroy"/>
0273	<RequestPayload>
0274	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0275	</RequestPayload>
0276	</BatchItem>
0277	</RequestMessage>
0278	<ResponseMessage>
0279	<ResponseHeader>
0280	<ProtocolVersion>
0281	<ProtocolVersionMajor type="Integer" value="1"/>
0282	<ProtocolVersionMinor type="Integer" value="0"/>
0283	</ProtocolVersion>
0284	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0285	<BatchCount type="Integer" value="1"/>
0286	</ResponseHeader>
0287	<BatchItem>
0288	<Operation type="Enumeration" value="Destroy"/>

0289	<ResultStatus type="Enumeration" value="OperationFailed"/>
0290	<ResultReason type="Enumeration" value="PermissionDenied"/>
0291	<ResultMessage type="TextString" value="DENIED"/>
0292	</BatchItem>
0293	</ResponseMessage>
	# TIME 6
0294	<RequestMessage>
0295	<RequestHeader>
0296	<ProtocolVersion>
0297	<ProtocolVersionMajor type="Integer" value="1"/>
0298	<ProtocolVersionMinor type="Integer" value="0"/>
0299	</ProtocolVersion>
0300	<BatchCount type="Integer" value="1"/>
0301	</RequestHeader>
0302	<BatchItem>
0303	<Operation type="Enumeration" value="Destroy"/>
0304	<RequestPayload>
0305	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0306	</RequestPayload>
0307	</BatchItem>
0308	</RequestMessage>
0309	<ResponseMessage>
0310	<ResponseHeader>
0311	<ProtocolVersion>
0312	<ProtocolVersionMajor type="Integer" value="1"/>
0313	<ProtocolVersionMinor type="Integer" value="0"/>
0314	</ProtocolVersion>
0315	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0316	<BatchCount type="Integer" value="1"/>
0317	</ResponseHeader>
0318	<BatchItem>
0319	<Operation type="Enumeration" value="Destroy"/>
0320	<ResultStatus type="Enumeration" value="Success"/>
0321	<ResponsePayload>
0322	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0323	</ResponsePayload>
0324	</BatchItem>
0325	</ResponseMessage>
	# TIME 7
0326	<RequestMessage>
0327	<RequestHeader>
0328	<ProtocolVersion>
0329	<ProtocolVersionMajor type="Integer" value="1"/>
0330	<ProtocolVersionMinor type="Integer" value="0"/>
0331	</ProtocolVersion>
0332	<BatchCount type="Integer" value="1"/>
0333	</RequestHeader>
0334	<BatchItem>
0335	<Operation type="Enumeration" value="Revoke"/>
0336	<RequestPayload>
0337	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0338	<RevocationReason>
0339	<RevocationReasonCode type="Enumeration" value="KeyCompromise"/>
0340	</RevocationReason>

0341	<CompromiseOccurrenceDate type="DateTime" value="1970-01-01T00:00:06+00:00"/>
0342	</RequestPayload>
0343	</BatchItem>
0344	</RequestMessage>
0345	<ResponseMessage>
0346	<ResponseHeader>
0347	<ProtocolVersion>
0348	<ProtocolVersionMajor type="Integer" value="1"/>
0349	<ProtocolVersionMinor type="Integer" value="0"/>
0350	</ProtocolVersion>
0351	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0352	<BatchCount type="Integer" value="1"/>
0353	</ResponseHeader>
0354	<BatchItem>
0355	<Operation type="Enumeration" value="Revoke"/>
0356	<ResultStatus type="Enumeration" value="Success"/>
0357	<ResponsePayload>
0358	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0359	</ResponsePayload>
0360	</BatchItem>
0361	</ResponseMessage>
0362	# TIME 8 <RequestMessage>
0363	<RequestHeader>
0364	<ProtocolVersion>
0365	<ProtocolVersionMajor type="Integer" value="1"/>
0366	<ProtocolVersionMinor type="Integer" value="0"/>
0367	</ProtocolVersion>
0368	<BatchCount type="Integer" value="1"/>
0369	</RequestHeader>
0370	<BatchItem>
0371	<Operation type="Enumeration" value="GetAttributes"/>
0372	<RequestPayload>
0373	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0374	<AttributeName type="TextString" value="State"/>
0375	</RequestPayload>
0376	</BatchItem>
0377	</RequestMessage>
0378	<ResponseMessage>
0379	<ResponseHeader>
0380	<ProtocolVersion>
0381	<ProtocolVersionMajor type="Integer" value="1"/>
0382	<ProtocolVersionMinor type="Integer" value="0"/>
0383	</ProtocolVersion>
0384	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0385	<BatchCount type="Integer" value="1"/>
0386	</ResponseHeader>
0387	<BatchItem>
0388	<Operation type="Enumeration" value="GetAttributes"/>
0389	<ResultStatus type="Enumeration" value="Success"/>
0390	<ResponsePayload>
0391	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0392	<Attribute>
0393	<AttributeName type="TextString" value="State"/>

0394	<AttributeValue type="Enumeration" value="Compromised"/>
0395	</Attribute>
0396	</ResponsePayload>
0397	</BatchItem>
0398	</ResponseMessage>
# TIME 9	
0399	<RequestMessage>
0400	<RequestHeader>
0401	<ProtocolVersion>
0402	<ProtocolVersionMajor type="Integer" value="1"/>
0403	<ProtocolVersionMinor type="Integer" value="0"/>
0404	</ProtocolVersion>
0405	<BatchCount type="Integer" value="1"/>
0406	</RequestHeader>
0407	<BatchItem>
0408	<Operation type="Enumeration" value="Destroy"/>
0409	<RequestPayload>
0410	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0411	</RequestPayload>
0412	</BatchItem>
0413	</RequestMessage>
0414	<ResponseMessage>
0415	<ResponseHeader>
0416	<ProtocolVersion>
0417	<ProtocolVersionMajor type="Integer" value="1"/>
0418	<ProtocolVersionMinor type="Integer" value="0"/>
0419	</ProtocolVersion>
0420	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0421	<BatchCount type="Integer" value="1"/>
0422	</ResponseHeader>
0423	<BatchItem>
0424	<Operation type="Enumeration" value="Destroy"/>
0425	<ResultStatus type="Enumeration" value="Success"/>
0426	<ResponsePayload>
0427	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0428	</ResponsePayload>
0429	</BatchItem>
0430	</ResponseMessage>

107

### 108 3.1.3 AKLC-M-3-10

109 CreateKeyPair, 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="CreateKeyPair"/>
0011	<RequestPayload>

```

0012     <CommonTemplateAttribute>
0013     <Attribute>
0014         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0015         <AttributeValue type="Enumeration" value="RSA"/>
0016     </Attribute>
0017     <Attribute>
0018         <AttributeName type="TextString" value="Cryptographic
Length"/>
0019         <AttributeValue type="Integer" value="2048"/>
0020     </Attribute>
0021 </CommonTemplateAttribute>
0022 <PrivateKeyTemplateAttribute>
0023 <Attribute>
0024     <AttributeName type="TextString" value="Name"/>
0025     <AttributeValue>
0026         <NameValue type="TextString" value="AKLC-M-3-10-
private"/>
0027         <NameType type="Enumeration"
value="UninterpretedTextString"/>
0028     </AttributeValue>
0029 </Attribute>
0030 <Attribute>
0031     <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0032     <AttributeValue type="Integer" value="Sign"/>
0033 </Attribute>
0034 </PrivateKeyTemplateAttribute>
0035 <PublicKeyTemplateAttribute>
0036 <Attribute>
0037     <AttributeName type="TextString" value="Name"/>
0038     <AttributeValue>
0039         <NameValue type="TextString" value="AKLC-M-3-10-
public"/>
0040         <NameType type="Enumeration"
value="UninterpretedTextString"/>
0041     </AttributeValue>
0042 </Attribute>
0043 <Attribute>
0044     <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0045     <AttributeValue type="Integer" value="Verify"/>
0046 </Attribute>
0047 </PublicKeyTemplateAttribute>
0048 </RequestPayload>
0049 </BatchItem>
0050 </RequestMessage>
0051 <ResponseMessage>
0052 <ResponseHeader>
0053     <ProtocolVersion>
0054         <ProtocolVersionMajor type="Integer" value="1"/>
0055         <ProtocolVersionMinor type="Integer" value="0"/>
0056     </ProtocolVersion>
0057     <TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/>
0058     <BatchCount type="Integer" value="1"/>
0059 </ResponseHeader>
0060 <BatchItem>
0061     <Operation type="Enumeration" value="CreateKeyPair"/>

```

0062	<ResultStatus type="Enumeration" value="Success"/>
0063	<ResponsePayload>
0064	<PrivateKeyUniqueIdentifier type="TextString"
0065	value="\$UNIQUE_IDENTIFIER_0"/>
0066	<PublicKeyUniqueIdentifier type="TextString"
0067	value="\$UNIQUE_IDENTIFIER_1"/>
0068	</ResponsePayload>
	</BatchItem>
	</ResponseMessage>
	# TIME 1
0069	<RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="0"/>
0074	</ProtocolVersion>
0075	<BatchCount type="Integer" value="1"/>
0076	</RequestHeader>
0077	<BatchItem>
0078	<Operation type="Enumeration" value="GetAttributes"/>
0079	<RequestPayload>
0080	<UniqueIdentifier type="TextString"
0081	value="\$UNIQUE_IDENTIFIER_0"/>
0082	<AttributeName type="TextString" value="State"/>
0083	<AttributeName type="TextString" value="Cryptographic Usage
0084	Mask"/>
0085	<AttributeName type="TextString" value="Unique Identifier"/>
0086	<AttributeName type="TextString" value="Object Type"/>
0087	<AttributeName type="TextString" value="Cryptographic
0088	Algorithm"/>
0089	<AttributeName type="TextString" value="Cryptographic
0090	Length"/>
0091	<AttributeName type="TextString" value="Digest"/>
0092	<AttributeName type="TextString" value="Initial Date"/>
0093	<AttributeName type="TextString" value="Last Change Date"/>
0094	</RequestPayload>
0095	</BatchItem>
0096	</RequestMessage>
0097	<ResponseMessage>
0098	<ResponseHeader>
0099	<ProtocolVersion>
0100	<ProtocolVersionMajor type="Integer" value="1"/>
0101	<ProtocolVersionMinor type="Integer" value="0"/>
0102	</ProtocolVersion>
0103	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0104	<BatchCount type="Integer" value="1"/>
0105	</ResponseHeader>
0106	<BatchItem>
0107	<Operation type="Enumeration" value="GetAttributes"/>
0108	<ResultStatus type="Enumeration" value="Success"/>
0109	<ResponsePayload>
0110	<UniqueIdentifier type="TextString"
0111	value="\$UNIQUE_IDENTIFIER_0"/>
	<Attribute>
	<AttributeName type="TextString" value="State"/>
	<AttributeValue type="Enumeration" value="PreActive"/>
	</Attribute>
	<Attribute>



```

0112     <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0113     <AttributeValue type="Integer" value="Sign"/>
0114     </Attribute>
0115     <Attribute>
0116         <AttributeName type="TextString" value="Unique Identifier"/>
0117         <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0118     </Attribute>
0119     <Attribute>
0120         <AttributeName type="TextString" value="Object Type"/>
0121         <AttributeValue type="Enumeration" value="PrivateKey"/>
0122     </Attribute>
0123     <Attribute>
0124         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0125         <AttributeValue type="Enumeration" value="RSA"/>
0126     </Attribute>
0127     <Attribute>
0128         <AttributeName type="TextString" value="Cryptographic
Length"/>
0129         <AttributeValue type="Integer" value="2048"/>
0130     </Attribute>
0131     <Attribute>
0132         <AttributeName type="TextString" value="Digest"/>
0133         <AttributeValue>
0134             <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0135             <DigestValue type="ByteString"
value="8eb422ae2b006a05d3c8a542a28536735241b6dc1c37926bc8007bd6220d9
230"/>
0136         </AttributeValue>
0137     </Attribute>
0138     <Attribute>
0139         <AttributeName type="TextString" value="Initial Date"/>
0140         <AttributeValue type="DateTime" value="2013-01-
11T08:18:21+00:00"/>
0141     </Attribute>
0142     <Attribute>
0143         <AttributeName type="TextString" value="Last Change Date"/>
0144         <AttributeValue type="DateTime" value="2013-01-
11T08:18:21+00:00"/>
0145     </Attribute>
0146     </ResponsePayload>
0147     </BatchItem>
0148     </ResponseMessage>
# TIME 2
0149     <RequestMessage>
0150         <RequestHeader>
0151             <ProtocolVersion>
0152                 <ProtocolVersionMajor type="Integer" value="1"/>
0153                 <ProtocolVersionMinor type="Integer" value="0"/>
0154             </ProtocolVersion>
0155             <BatchCount type="Integer" value="1"/>
0156         </RequestHeader>
0157     <BatchItem>
0158         <Operation type="Enumeration" value="Activate"/>
0159     <RequestPayload>
0160         <UniqueIdentifier type="TextString"

```

0161	value="\$UNIQUE_IDENTIFIER_0"/>
0162	</RequestPayload>
0163	</BatchItem>
0164	</RequestMessage>
0164	<ResponseMessage>
0165	<ResponseHeader>
0166	<ProtocolVersion>
0167	<ProtocolVersionMajor type="Integer" value="1"/>
0168	<ProtocolVersionMinor type="Integer" value="0"/>
0169	</ProtocolVersion>
0170	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0171	<BatchCount type="Integer" value="1"/>
0172	</ResponseHeader>
0173	<BatchItem>
0174	<Operation type="Enumeration" value="Activate"/>
0175	<ResultStatus type="Enumeration" value="Success"/>
0176	<ResponsePayload>
0177	<UniqueIdentifier type="TextString"
0178	value="\$UNIQUE_IDENTIFIER_0"/>
0179	</ResponsePayload>
0180	</BatchItem>
0180	</ResponseMessage>
0181	# TIME 3
0181	<RequestMessage>
0182	<RequestHeader>
0183	<ProtocolVersion>
0184	<ProtocolVersionMajor type="Integer" value="1"/>
0185	<ProtocolVersionMinor type="Integer" value="0"/>
0186	</ProtocolVersion>
0187	<BatchCount type="Integer" value="1"/>
0188	</RequestHeader>
0189	<BatchItem>
0190	<Operation type="Enumeration" value="GetAttributes"/>
0191	<RequestPayload>
0192	<UniqueIdentifier type="TextString"
0193	value="\$UNIQUE_IDENTIFIER_0"/>
0194	<AttributeName type="TextString" value="State"/>
0195	<AttributeName type="TextString" value="Activation Date"/>
0196	<AttributeName type="TextString" value="Deactivation Date"/>
0197	</RequestPayload>
0198	</BatchItem>
0198	</RequestMessage>
0199	<ResponseMessage>
0200	<ResponseHeader>
0201	<ProtocolVersion>
0202	<ProtocolVersionMajor type="Integer" value="1"/>
0203	<ProtocolVersionMinor type="Integer" value="0"/>
0204	</ProtocolVersion>
0205	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0206	<BatchCount type="Integer" value="1"/>
0207	</ResponseHeader>
0208	<BatchItem>
0209	<Operation type="Enumeration" value="GetAttributes"/>
0210	<ResultStatus type="Enumeration" value="Success"/>
0211	<ResponsePayload>
0212	<UniqueIdentifier type="TextString"
0213	value="\$UNIQUE_IDENTIFIER_0"/>
0213	<Attribute>

0214	<AttributeName type="TextString" value="State"/>
0215	<AttributeValue type="Enumeration" value="Active"/>
0216	</Attribute>
0217	<Attribute>
0218	<AttributeName type="TextString" value="Activation Date"/>
0219	<AttributeValue type="DateTime" value="2013-01-10T23:36:01+00:00"/>
0220	</Attribute>
0221	</ResponsePayload>
0222	</BatchItem>
0223	</ResponseMessage>
	# TIME 4
0224	<RequestMessage>
0225	<RequestHeader>
0226	<ProtocolVersion>
0227	<ProtocolVersionMajor type="Integer" value="1"/>
0228	<ProtocolVersionMinor type="Integer" value="0"/>
0229	</ProtocolVersion>
0230	<BatchCount type="Integer" value="1"/>
0231	</RequestHeader>
0232	<BatchItem>
0233	<Operation type="Enumeration" value="ModifyAttribute"/>
0234	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0235	<RequestPayload>
0236	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0237	<Attribute>
0238	<AttributeName type="TextString" value="Activation Date"/>
0239	<AttributeValue type="DateTime" value="\$NOW"/>
0240	</Attribute>
0241	</RequestPayload>
0242	</BatchItem>
0243	</RequestMessage>
0244	<ResponseMessage>
0245	<ResponseHeader>
0246	<ProtocolVersion>
0247	<ProtocolVersionMajor type="Integer" value="1"/>
0248	<ProtocolVersionMinor type="Integer" value="0"/>
0249	</ProtocolVersion>
0250	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0251	<BatchCount type="Integer" value="1"/>
0252	</ResponseHeader>
0253	<BatchItem>
0254	<Operation type="Enumeration" value="ModifyAttribute"/>
0255	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0256	<ResultStatus type="Enumeration" value="OperationFailed"/>
0257	<ResultReason type="Enumeration" value="PermissionDenied"/>
0258	<ResultMessage type="TextString" value="DENIED"/>
0259	</BatchItem>
0260	</ResponseMessage>
	# TIME 5
0261	<RequestMessage>
0262	<RequestHeader>
0263	<ProtocolVersion>
0264	<ProtocolVersionMajor type="Integer" value="1"/>
0265	<ProtocolVersionMinor type="Integer" value="0"/>
0266	</ProtocolVersion>
0267	<BatchCount type="Integer" value="1"/>

0268	</RequestHeader>
0269	<BatchItem>
0270	<Operation type="Enumeration" value="Revoke"/>
0271	<RequestPayload>
0272	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0273	<RevocationReason>
0274	<RevocationReasonCode type="Enumeration" value="KeyCompromise"/>
0275	</RevocationReason>
0276	<CompromiseOccurrenceDate type="DateTime" value="1970-01- 01T00:00:06+00:00"/>
0277	</RequestPayload>
0278	</BatchItem>
0279	</RequestMessage>
0280	<ResponseMessage>
0281	<ResponseHeader>
0282	<ProtocolVersion>
0283	<ProtocolVersionMajor type="Integer" value="1"/>
0284	<ProtocolVersionMinor type="Integer" value="0"/>
0285	</ProtocolVersion>
0286	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0287	<BatchCount type="Integer" value="1"/>
0288	</ResponseHeader>
0289	<BatchItem>
0290	<Operation type="Enumeration" value="Revoke"/>
0291	<ResultStatus type="Enumeration" value="Success"/>
0292	<ResponsePayload>
0293	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0294	</ResponsePayload>
0295	</BatchItem>
0296	</ResponseMessage>
	# TIME 6
0297	<RequestMessage>
0298	<RequestHeader>
0299	<ProtocolVersion>
0300	<ProtocolVersionMajor type="Integer" value="1"/>
0301	<ProtocolVersionMinor type="Integer" value="0"/>
0302	</ProtocolVersion>
0303	<BatchCount type="Integer" value="1"/>
0304	</RequestHeader>
0305	<BatchItem>
0306	<Operation type="Enumeration" value="GetAttributes"/>
0307	<RequestPayload>
0308	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0309	<AttributeName type="TextString" value="State"/>
0310	</RequestPayload>
0311	</BatchItem>
0312	</RequestMessage>
0313	<ResponseMessage>
0314	<ResponseHeader>
0315	<ProtocolVersion>
0316	<ProtocolVersionMajor type="Integer" value="1"/>
0317	<ProtocolVersionMinor type="Integer" value="0"/>
0318	</ProtocolVersion>
0319	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>

0320	<BatchCount type="Integer" value="1"/>
0321	</ResponseHeader>
0322	<BatchItem>
0323	<Operation type="Enumeration" value="GetAttributes"/>
0324	<ResultStatus type="Enumeration" value="Success"/>
0325	<ResponsePayload>
0326	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0327	<Attribute>
0328	<AttributeName type="TextString" value="State"/>
0329	<AttributeValue type="Enumeration" value="Compromised"/>
0330	</Attribute>
0331	</ResponsePayload>
0332	</BatchItem>
0333	</ResponseMessage>
	# TIME 7
0334	<RequestMessage>
0335	<RequestHeader>
0336	<ProtocolVersion>
0337	<ProtocolVersionMajor type="Integer" value="1"/>
0338	<ProtocolVersionMinor type="Integer" value="0"/>
0339	</ProtocolVersion>
0340	<BatchCount type="Integer" value="1"/>
0341	</RequestHeader>
0342	<BatchItem>
0343	<Operation type="Enumeration" value="GetAttributes"/>
0344	<RequestPayload>
0345	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0346	<AttributeName type="TextString" value="State"/>
0347	</RequestPayload>
0348	</BatchItem>
0349	</RequestMessage>
0350	<ResponseMessage>
0351	<ResponseHeader>
0352	<ProtocolVersion>
0353	<ProtocolVersionMajor type="Integer" value="1"/>
0354	<ProtocolVersionMinor type="Integer" value="0"/>
0355	</ProtocolVersion>
0356	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0357	<BatchCount type="Integer" value="1"/>
0358	</ResponseHeader>
0359	<BatchItem>
0360	<Operation type="Enumeration" value="GetAttributes"/>
0361	<ResultStatus type="Enumeration" value="Success"/>
0362	<ResponsePayload>
0363	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0364	<Attribute>
0365	<AttributeName type="TextString" value="State"/>
0366	<AttributeValue type="Enumeration" value="PreActive"/>
0367	</Attribute>
0368	</ResponsePayload>
0369	</BatchItem>
0370	</ResponseMessage>
	# TIME 8
0371	<RequestMessage>
0372	<RequestHeader>

0373	<ProtocolVersion>
0374	<ProtocolVersionMajor type="Integer" value="1"/>
0375	<ProtocolVersionMinor type="Integer" value="0"/>
0376	</ProtocolVersion>
0377	<BatchCount type="Integer" value="1"/>
0378	</RequestHeader>
0379	<BatchItem>
0380	<Operation type="Enumeration" value="Destroy"/>
0381	<RequestPayload>
0382	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0383	</RequestPayload>
0384	</BatchItem>
0385	</RequestMessage>
0386	<ResponseMessage>
0387	<ResponseHeader>
0388	<ProtocolVersion>
0389	<ProtocolVersionMajor type="Integer" value="1"/>
0390	<ProtocolVersionMinor type="Integer" value="0"/>
0391	</ProtocolVersion>
0392	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0393	<BatchCount type="Integer" value="1"/>
0394	</ResponseHeader>
0395	<BatchItem>
0396	<Operation type="Enumeration" value="Destroy"/>
0397	<ResultStatus type="Enumeration" value="Success"/>
0398	<ResponsePayload>
0399	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0400	</ResponsePayload>
0401	</BatchItem>
0402	</ResponseMessage>
	<i># TIME 9</i>
0403	<RequestMessage>
0404	<RequestHeader>
0405	<ProtocolVersion>
0406	<ProtocolVersionMajor type="Integer" value="1"/>
0407	<ProtocolVersionMinor type="Integer" value="0"/>
0408	</ProtocolVersion>
0409	<BatchCount type="Integer" value="1"/>
0410	</RequestHeader>
0411	<BatchItem>
0412	<Operation type="Enumeration" value="Destroy"/>
0413	<RequestPayload>
0414	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0415	</RequestPayload>
0416	</BatchItem>
0417	</RequestMessage>
0418	<ResponseMessage>
0419	<ResponseHeader>
0420	<ProtocolVersion>
0421	<ProtocolVersionMajor type="Integer" value="1"/>
0422	<ProtocolVersionMinor type="Integer" value="0"/>
0423	</ProtocolVersion>
0424	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0425	<BatchCount type="Integer" value="1"/>
0426	</ResponseHeader>

```

0427 <BatchItem>
0428   <Operation type="Enumeration" value="Destroy"/>
0429   <ResultStatus type="Enumeration" value="Success"/>
0430   <ResponsePayload>
0431     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0432   </ResponsePayload>
0433 </BatchItem>
0434 </ResponseMessage>

```

110

## 111 3.2 Mandatory Test Cases KMIP v1.1

### 112 3.2.1 AKLC-M-1-11

113 CreateKeyPair, GetAttributes, 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="CreateKeyPair"/>
0011     <RequestPayload>
0012       <CommonTemplateAttribute>
0013         <Attribute>
0014           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0015           <AttributeValue type="Enumeration" value="RSA"/>
0016         </Attribute>
0017         <Attribute>
0018           <AttributeName type="TextString" value="Cryptographic
Length"/>
0019           <AttributeValue type="Integer" value="2048"/>
0020         </Attribute>
0021       </CommonTemplateAttribute>
0022       <PrivateKeyTemplateAttribute>
0023         <Attribute>
0024           <AttributeName type="TextString" value="Name"/>
0025           <AttributeValue>
0026             <NameValue type="TextString" value="AKLC-M-1-11-
private"/>
0027             <NameType type="Enumeration"
value="UninterpretedTextString"/>
0028           </AttributeValue>
0029         </Attribute>
0030         <Attribute>
0031           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0032           <AttributeValue type="Integer" value="Sign"/>
0033         </Attribute>
0034       </PrivateKeyTemplateAttribute>
0035       <PublicKeyTemplateAttribute>

```

0036	<Attribute>
0037	<AttributeName type="TextString" value="Name"/>
0038	<AttributeValue>
0039	<NameValue type="TextString" value="AKLC-M-1-11- public"/>
0040	<NameType type="Enumeration" value="UninterpretedTextString"/>
0041	</AttributeValue>
0042	</Attribute>
0043	<Attribute>
0044	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0045	<AttributeValue type="Integer" value="Verify"/>
0046	</Attribute>
0047	</PublicKeyTemplateAttribute>
0048	</RequestPayload>
0049	</BatchItem>
0050	</RequestMessage>
0051	<ResponseMessage>
0052	<ResponseHeader>
0053	<ProtocolVersion>
0054	<ProtocolVersionMajor type="Integer" value="1"/>
0055	<ProtocolVersionMinor type="Integer" value="1"/>
0056	</ProtocolVersion>
0057	<TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/>
0058	<BatchCount type="Integer" value="1"/>
0059	</ResponseHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="CreateKeyPair"/>
0062	<ResultStatus type="Enumeration" value="Success"/>
0063	<ResponsePayload>
0064	<PrivateKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0065	<PublicKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
0069	# TIME 1 <RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="1"/>
0074	</ProtocolVersion>
0075	<BatchCount type="Integer" value="1"/>
0076	</RequestHeader>
0077	<BatchItem>
0078	<Operation type="Enumeration" value="GetAttributes"/>
0079	<RequestPayload>
0080	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0081	<AttributeName type="TextString" value="State"/>
0082	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0083	<AttributeName type="TextString" value="Unique Identifier"/>
0084	<AttributeName type="TextString" value="Object Type"/>
0085	<AttributeName type="TextString" value="Cryptographic



0086	Algorithm"/> <AttributeName type="TextString" value="Cryptographic Length"/>
0087	<AttributeName type="TextString" value="Digest"/>
0088	<AttributeName type="TextString" value="Initial Date"/>
0089	<AttributeName type="TextString" value="Last Change Date"/>
0090	<AttributeName type="TextString" value="Activation Date"/>
0091	</RequestPayload>
0092	</BatchItem>
0093	</RequestMessage>
0094	<ResponseMessage>
0095	<ResponseHeader>
0096	<ProtocolVersion>
0097	<ProtocolVersionMajor type="Integer" value="1"/>
0098	<ProtocolVersionMinor type="Integer" value="1"/>
0099	</ProtocolVersion>
0100	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0101	<BatchCount type="Integer" value="1"/>
0102	</ResponseHeader>
0103	<BatchItem>
0104	<Operation type="Enumeration" value="GetAttributes"/>
0105	<ResultStatus type="Enumeration" value="Success"/>
0106	<ResponsePayload>
0107	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0108	<Attribute>
0109	<AttributeName type="TextString" value="State"/>
0110	<AttributeValue type="Enumeration" value="PreActive"/>
0111	</Attribute>
0112	<Attribute>
0113	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0114	<AttributeValue type="Integer" value="Sign"/>
0115	</Attribute>
0116	<Attribute>
0117	<AttributeName type="TextString" value="Unique Identifier"/>
0118	<AttributeValue type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0119	</Attribute>
0120	<Attribute>
0121	<AttributeName type="TextString" value="Object Type"/>
0122	<AttributeValue type="Enumeration" value="PrivateKey"/>
0123	</Attribute>
0124	<Attribute>
0125	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0126	<AttributeValue type="Enumeration" value="RSA"/>
0127	</Attribute>
0128	<Attribute>
0129	<AttributeName type="TextString" value="Cryptographic Length"/>
0130	<AttributeValue type="Integer" value="2048"/>
0131	</Attribute>
0132	<Attribute>
0133	<AttributeName type="TextString" value="Digest"/>
0134	<AttributeValue>
0135	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0136	<DigestValue type="ByteString">

0137	value="8eb422ae2b006a05d3c8a542a28536735241b6dc1c37926bc8007bd6220d9230"/>
0138	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0139	</AttributeValue>
0140	</Attribute>
0141	<Attribute>
0142	<AttributeName type="TextString" value="Initial Date"/>
0143	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0144	</Attribute>
0145	<AttributeName type="TextString" value="Last Change Date"/>
0146	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0147	</Attribute>
0148	</ResponsePayload>
0149	</BatchItem>
0150	</ResponseMessage>
0151	# TIME 2 <RequestMessage>
0152	<RequestHeader>
0153	<ProtocolVersion>
0154	<ProtocolVersionMajor type="Integer" value="1"/>
0155	<ProtocolVersionMinor type="Integer" value="1"/>
0156	</ProtocolVersion>
0157	<BatchCount type="Integer" value="1"/>
0158	</RequestHeader>
0159	<BatchItem>
0160	<Operation type="Enumeration" value="GetAttributes"/>
0161	<RequestPayload>
0162	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0163	<AttributeName type="TextString" value="State"/>
0164	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0165	<AttributeName type="TextString" value="Unique Identifier"/>
0166	<AttributeName type="TextString" value="Object Type"/>
0167	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0168	<AttributeName type="TextString" value="Cryptographic Length"/>
0169	<AttributeName type="TextString" value="Digest"/>
0170	<AttributeName type="TextString" value="Initial Date"/>
0171	<AttributeName type="TextString" value="Last Change Date"/>
0172	<AttributeName type="TextString" value="Activation Date"/>
0173	</RequestPayload>
0174	</BatchItem>
0175	</RequestMessage>
0176	<ResponseMessage>
0177	<ResponseHeader>
0178	<ProtocolVersion>
0179	<ProtocolVersionMajor type="Integer" value="1"/>
0180	<ProtocolVersionMinor type="Integer" value="1"/>
0181	</ProtocolVersion>
0182	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0183	<BatchCount type="Integer" value="1"/>
0184	</ResponseHeader>
0185	<BatchItem>

0186	<Operation type="Enumeration" value="GetAttributes"/>
0187	<ResultStatus type="Enumeration" value="Success"/>
0188	<ResponsePayload>
0189	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0190	<Attribute>
0191	<AttributeName type="TextString" value="State"/>
0192	<AttributeValue type="Enumeration" value="PreActive"/>
0193	</Attribute>
0194	<Attribute>
0195	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0196	<AttributeValue type="Integer" value="Verify"/>
0197	</Attribute>
0198	<Attribute>
0199	<AttributeName type="TextString" value="Unique Identifier"/>
0200	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0201	</Attribute>
0202	<Attribute>
0203	<AttributeName type="TextString" value="Object Type"/>
0204	<AttributeValue type="Enumeration" value="PublicKey"/>
0205	</Attribute>
0206	<Attribute>
0207	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0208	<AttributeValue type="Enumeration" value="RSA"/>
0209	</Attribute>
0210	<Attribute>
0211	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0212	<AttributeValue type="Integer" value="2048"/>
0213	</Attribute>
0214	<Attribute>
0215	<AttributeName type="TextString" value="Digest"/>
0216	<AttributeValue>
0217	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0218	<DigestValue type="ByteString"
	value="82bcff8afab753809db804e654013ded708c3996a50c6ce9313f9b3915442
	ce9"/>
0219	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0220	</AttributeValue>
0221	</Attribute>
0222	<Attribute>
0223	<AttributeName type="TextString" value="Initial Date"/>
0224	<AttributeValue type="DateTime" value="2013-01-
	11T08:19:49+00:00"/>
0225	</Attribute>
0226	<Attribute>
0227	<AttributeName type="TextString" value="Last Change Date"/>
0228	<AttributeValue type="DateTime" value="2013-01-
	11T08:19:49+00:00"/>
0229	</Attribute>
0230	</ResponsePayload>
0231	</BatchItem>
0232	</ResponseMessage>
0233	# TIME 3 <RequestMessage>

0234	<RequestHeader>
0235	<ProtocolVersion>
0236	<ProtocolVersionMajor type="Integer" value="1"/>
0237	<ProtocolVersionMinor type="Integer" value="1"/>
0238	</ProtocolVersion>
0239	<BatchCount type="Integer" value="1"/>
0240	</RequestHeader>
0241	<BatchItem>
0242	<Operation type="Enumeration" value="Destroy"/>
0243	<RequestPayload>
0244	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0245	</RequestPayload>
0246	</BatchItem>
0247	</RequestMessage>
0248	<ResponseMessage>
0249	<ResponseHeader>
0250	<ProtocolVersion>
0251	<ProtocolVersionMajor type="Integer" value="1"/>
0252	<ProtocolVersionMinor type="Integer" value="1"/>
0253	</ProtocolVersion>
0254	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0255	<BatchCount type="Integer" value="1"/>
0256	</ResponseHeader>
0257	<BatchItem>
0258	<Operation type="Enumeration" value="Destroy"/>
0259	<ResultStatus type="Enumeration" value="Success"/>
0260	<ResponsePayload>
0261	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0262	</ResponsePayload>
0263	</BatchItem>
0264	</ResponseMessage>
	# TIME 4
0265	<RequestMessage>
0266	<RequestHeader>
0267	<ProtocolVersion>
0268	<ProtocolVersionMajor type="Integer" value="1"/>
0269	<ProtocolVersionMinor type="Integer" value="1"/>
0270	</ProtocolVersion>
0271	<BatchCount type="Integer" value="1"/>
0272	</RequestHeader>
0273	<BatchItem>
0274	<Operation type="Enumeration" value="Destroy"/>
0275	<RequestPayload>
0276	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0277	</RequestPayload>
0278	</BatchItem>
0279	</RequestMessage>
0280	<ResponseMessage>
0281	<ResponseHeader>
0282	<ProtocolVersion>
0283	<ProtocolVersionMajor type="Integer" value="1"/>
0284	<ProtocolVersionMinor type="Integer" value="1"/>
0285	</ProtocolVersion>
0286	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0287	<BatchCount type="Integer" value="1"/>

```

0288 </ResponseHeader>
0289 <BatchItem>
0290   <Operation type="Enumeration" value="Destroy"/>
0291   <ResultStatus type="Enumeration" value="Success"/>
0292   <ResponsePayload>
0293     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0294   </ResponsePayload>
0295 </BatchItem>
0296 </ResponseMessage>

```

114

### 115 3.2.2 AKLC-M-2-11

116 CreateKeyPair, 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="CreateKeyPair"/>
0011     <RequestPayload>
0012       <CommonTemplateAttribute>
0013         <Attribute>
0014           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0015           <AttributeValue type="Enumeration" value="RSA"/>
0016         </Attribute>
0017         <Attribute>
0018           <AttributeName type="TextString" value="Cryptographic
Length"/>
0019           <AttributeValue type="Integer" value="2048"/>
0020         </Attribute>
0021       </CommonTemplateAttribute>
0022       <PrivateKeyTemplateAttribute>
0023         <Attribute>
0024           <AttributeName type="TextString" value="Name"/>
0025           <AttributeValue>
0026             <NameValue type="TextString" value="AKLC-M-2-11-
private"/>
0027             <NameType type="Enumeration"
value="UninterpretedTextString"/>
0028           </AttributeValue>
0029         </Attribute>
0030         <Attribute>
0031           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0032           <AttributeValue type="Integer" value="Sign"/>
0033         </Attribute>
0034       </PrivateKeyTemplateAttribute>
0035       <PublicKeyTemplateAttribute>
0036         <Attribute>

```

0037	<AttributeName type="TextString" value="Name"/>
0038	<AttributeValue>
0039	<NameValue type="TextString" value="AKLC-M-2-11-
0040	public"/>
0041	<NameType type="Enumeration"
0042	value="UninterpretedTextString"/>
0043	</AttributeValue>
0044	</Attribute>
0045	<AttributeName type="TextString" value="Cryptographic
0046	Usage Mask"/>
0047	<AttributeValue type="Integer" value="Verify"/>
0048	</Attribute>
0049	</PublicKeyTemplateAttribute>
0050	</RequestPayload>
0051	</BatchItem>
0052	</RequestMessage>
0053	<ResponseMessage>
0054	<ResponseHeader>
0055	<ProtocolVersion>
0056	<ProtocolVersionMajor type="Integer" value="1"/>
0057	<ProtocolVersionMinor type="Integer" value="1"/>
0058	</ProtocolVersion>
0059	<TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/>
0060	<BatchCount type="Integer" value="1"/>
0061	</ResponseHeader>
0062	<BatchItem>
0063	<Operation type="Enumeration" value="CreateKeyPair"/>
0064	<ResultStatus type="Enumeration" value="Success"/>
0065	<ResponsePayload>
0066	<PrivateKeyUniqueIdentifier type="TextString"
0067	value="\$UNIQUE_IDENTIFIER_0"/>
0068	<PublicKeyUniqueIdentifier type="TextString"
0069	value="\$UNIQUE_IDENTIFIER_1"/>
0070	</ResponsePayload>
0071	</BatchItem>
0072	</ResponseMessage>
0073	# TIME 1
0074	<RequestMessage>
0075	<RequestHeader>
0076	<ProtocolVersion>
0077	<ProtocolVersionMajor type="Integer" value="1"/>
0078	<ProtocolVersionMinor type="Integer" value="1"/>
0079	</ProtocolVersion>
0080	<BatchCount type="Integer" value="1"/>
0081	</RequestHeader>
0082	<BatchItem>
0083	<Operation type="Enumeration" value="GetAttributes"/>
0084	<RequestPayload>
0085	<UniqueIdentifier type="TextString"
0086	value="\$UNIQUE_IDENTIFIER_0"/>
0087	<AttributeName type="TextString" value="State"/>
0088	<AttributeName type="TextString" value="Cryptographic Usage
0089	Mask"/>
0090	<AttributeName type="TextString" value="Unique Identifier"/>
0091	<AttributeName type="TextString" value="Object Type"/>
0092	<AttributeName type="TextString" value="Cryptographic
0093	Algorithm"/>

```

0086     <AttributeName type="TextString" value="Cryptographic
Length"/>
0087     <AttributeName type="TextString" value="Digest"/>
0088     <AttributeName type="TextString" value="Initial Date"/>
0089     <AttributeName type="TextString" value="Last Change Date"/>
0090     </RequestPayload>
0091     </BatchItem>
0092 </RequestMessage>
0093 <ResponseMessage>
0094   <ResponseHeader>
0095     <ProtocolVersion>
0096       <ProtocolVersionMajor type="Integer" value="1"/>
0097       <ProtocolVersionMinor type="Integer" value="1"/>
0098     </ProtocolVersion>
0099     <TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0100     <BatchCount type="Integer" value="1"/>
0101   </ResponseHeader>
0102   <BatchItem>
0103     <Operation type="Enumeration" value="GetAttributes"/>
0104     <ResultStatus type="Enumeration" value="Success"/>
0105     <ResponsePayload>
0106       <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0107       <Attribute>
0108         <AttributeName type="TextString" value="State"/>
0109         <AttributeValue type="Enumeration" value="PreActive"/>
0110       </Attribute>
0111       <Attribute>
0112         <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0113         <AttributeValue type="Integer" value="Sign"/>
0114       </Attribute>
0115       <Attribute>
0116         <AttributeName type="TextString" value="Unique Identifier"/>
0117         <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0118       </Attribute>
0119       <Attribute>
0120         <AttributeName type="TextString" value="Object Type"/>
0121         <AttributeValue type="Enumeration" value="PrivateKey"/>
0122       </Attribute>
0123       <Attribute>
0124         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0125         <AttributeValue type="Enumeration" value="RSA"/>
0126       </Attribute>
0127       <Attribute>
0128         <AttributeName type="TextString" value="Cryptographic
Length"/>
0129         <AttributeValue type="Integer" value="2048"/>
0130       </Attribute>
0131       <Attribute>
0132         <AttributeName type="TextString" value="Digest"/>
0133         <AttributeValue>
0134           <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0135           <DigestValue type="ByteString"
value="8eb422ae2b006a05d3c8a542a28536735241b6dc1c37926bc8007bd6220d9
230"/>

```

0136	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0137	</AttributeValue>
0138	</Attribute>
0139	<Attribute>
0140	<AttributeName type="TextString" value="Initial Date"/>
0141	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0142	</Attribute>
0143	<Attribute>
0144	<AttributeName type="TextString" value="Last Change Date"/>
0145	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0146	</Attribute>
0147	</ResponsePayload>
0148	</BatchItem>
0149	</ResponseMessage>
	# TIME 2
0150	<RequestMessage>
0151	<RequestHeader>
0152	<ProtocolVersion>
0153	<ProtocolVersionMajor type="Integer" value="1"/>
0154	<ProtocolVersionMinor type="Integer" value="1"/>
0155	</ProtocolVersion>
0156	<BatchCount type="Integer" value="1"/>
0157	</RequestHeader>
0158	<BatchItem>
0159	<Operation type="Enumeration" value="Activate"/>
0160	<RequestPayload>
0161	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0162	</RequestPayload>
0163	</BatchItem>
0164	</RequestMessage>
0165	<ResponseMessage>
0166	<ResponseHeader>
0167	<ProtocolVersion>
0168	<ProtocolVersionMajor type="Integer" value="1"/>
0169	<ProtocolVersionMinor type="Integer" value="1"/>
0170	</ProtocolVersion>
0171	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0172	<BatchCount type="Integer" value="1"/>
0173	</ResponseHeader>
0174	<BatchItem>
0175	<Operation type="Enumeration" value="Activate"/>
0176	<ResultStatus type="Enumeration" value="Success"/>
0177	<ResponsePayload>
0178	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0179	</ResponsePayload>
0180	</BatchItem>
0181	</ResponseMessage>
	# TIME 3
0182	<RequestMessage>
0183	<RequestHeader>
0184	<ProtocolVersion>
0185	<ProtocolVersionMajor type="Integer" value="1"/>
0186	<ProtocolVersionMinor type="Integer" value="1"/>
0187	</ProtocolVersion>



0188	<BatchCount type="Integer" value="1"/>
0189	</RequestHeader>
0190	<BatchItem>
0191	<Operation type="Enumeration" value="GetAttributes"/>
0192	<RequestPayload>
0193	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0194	<AttributeName type="TextString" value="State"/>
0195	<AttributeName type="TextString" value="Activation Date"/>
0196	<AttributeName type="TextString" value="Deactivation Date"/>
0197	</RequestPayload>
0198	</BatchItem>
0199	</RequestMessage>
0200	<ResponseMessage>
0201	<ResponseHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="1"/>
0205	</ProtocolVersion>
0206	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0207	<BatchCount type="Integer" value="1"/>
0208	</ResponseHeader>
0209	<BatchItem>
0210	<Operation type="Enumeration" value="GetAttributes"/>
0211	<ResultStatus type="Enumeration" value="Success"/>
0212	<ResponsePayload>
0213	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0214	<Attribute>
0215	<AttributeName type="TextString" value="State"/>
0216	<AttributeValue type="Enumeration" value="Active"/>
0217	</Attribute>
0218	<Attribute>
0219	<AttributeName type="TextString" value="Activation Date"/>
0220	<AttributeValue type="DateTime" value="2013-01- 10T23:36:01+00:00"/>
0221	</Attribute>
0222	</ResponsePayload>
0223	</BatchItem>
0224	</ResponseMessage>
	# TIME 4
0225	<RequestMessage>
0226	<RequestHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="1"/>
0230	</ProtocolVersion>
0231	<BatchCount type="Integer" value="1"/>
0232	</RequestHeader>
0233	<BatchItem>
0234	<Operation type="Enumeration" value="GetAttributes"/>
0235	<RequestPayload>
0236	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0237	<AttributeName type="TextString" value="State"/>
0238	<AttributeName type="TextString" value="Activation Date"/>
0239	<AttributeName type="TextString" value="Deactivation Date"/>
0240	</RequestPayload>

0241	</BatchItem>
0242	</RequestMessage>
0243	<ResponseMessage>
0244	<ResponseHeader>
0245	<ProtocolVersion>
0246	<ProtocolVersionMajor type="Integer" value="1"/>
0247	<ProtocolVersionMinor type="Integer" value="1"/>
0248	</ProtocolVersion>
0249	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0250	<BatchCount type="Integer" value="1"/>
0251	</ResponseHeader>
0252	<BatchItem>
0253	<Operation type="Enumeration" value="GetAttributes"/>
0254	<ResultStatus type="Enumeration" value="Success"/>
0255	<ResponsePayload>
0256	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0257	<Attribute>
0258	<AttributeName type="TextString" value="State"/>
0259	<AttributeValue type="Enumeration" value="PreActive"/>
0260	</Attribute>
0261	</ResponsePayload>
0262	</BatchItem>
0263	</ResponseMessage>
	# TIME 5
0264	<RequestMessage>
0265	<RequestHeader>
0266	<ProtocolVersion>
0267	<ProtocolVersionMajor type="Integer" value="1"/>
0268	<ProtocolVersionMinor type="Integer" value="1"/>
0269	</ProtocolVersion>
0270	<BatchCount type="Integer" value="1"/>
0271	</RequestHeader>
0272	<BatchItem>
0273	<Operation type="Enumeration" value="Destroy"/>
0274	<RequestPayload>
0275	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0276	</RequestPayload>
0277	</BatchItem>
0278	</RequestMessage>
0279	<ResponseMessage>
0280	<ResponseHeader>
0281	<ProtocolVersion>
0282	<ProtocolVersionMajor type="Integer" value="1"/>
0283	<ProtocolVersionMinor type="Integer" value="1"/>
0284	</ProtocolVersion>
0285	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0286	<BatchCount type="Integer" value="1"/>
0287	</ResponseHeader>
0288	<BatchItem>
0289	<Operation type="Enumeration" value="Destroy"/>
0290	<ResultStatus type="Enumeration" value="OperationFailed"/>
0291	<ResultReason type="Enumeration" value="PermissionDenied"/>
0292	<ResultMessage type="TextString" value="DENIED"/>
0293	</BatchItem>
0294	</ResponseMessage>
	# TIME 6

0295	<RequestMessage>
0296	<RequestHeader>
0297	<ProtocolVersion>
0298	<ProtocolVersionMajor type="Integer" value="1"/>
0299	<ProtocolVersionMinor type="Integer" value="1"/>
0300	</ProtocolVersion>
0301	<BatchCount type="Integer" value="1"/>
0302	</RequestHeader>
0303	<BatchItem>
0304	<Operation type="Enumeration" value="Destroy"/>
0305	<RequestPayload>
0306	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0307	</RequestPayload>
0308	</BatchItem>
0309	</RequestMessage>
0310	<ResponseMessage>
0311	<ResponseHeader>
0312	<ProtocolVersion>
0313	<ProtocolVersionMajor type="Integer" value="1"/>
0314	<ProtocolVersionMinor type="Integer" value="1"/>
0315	</ProtocolVersion>
0316	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0317	<BatchCount type="Integer" value="1"/>
0318	</ResponseHeader>
0319	<BatchItem>
0320	<Operation type="Enumeration" value="Destroy"/>
0321	<ResultStatus type="Enumeration" value="Success"/>
0322	<ResponsePayload>
0323	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0324	</ResponsePayload>
0325	</BatchItem>
0326	</ResponseMessage>
	# TIME 7
0327	<RequestMessage>
0328	<RequestHeader>
0329	<ProtocolVersion>
0330	<ProtocolVersionMajor type="Integer" value="1"/>
0331	<ProtocolVersionMinor type="Integer" value="1"/>
0332	</ProtocolVersion>
0333	<BatchCount type="Integer" value="1"/>
0334	</RequestHeader>
0335	<BatchItem>
0336	<Operation type="Enumeration" value="Revoke"/>
0337	<RequestPayload>
0338	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0339	<RevocationReason>
0340	<RevocationReasonCode type="Enumeration"
	value="KeyCompromise"/>
0341	</RevocationReason>
0342	<CompromiseOccurrenceDate type="DateTime" value="1970-01-
	01T00:00:06+00:00"/>
0343	</RequestPayload>
0344	</BatchItem>
0345	</RequestMessage>
0346	<ResponseMessage>

0347	<ResponseHeader>
0348	<ProtocolVersion>
0349	<ProtocolVersionMajor type="Integer" value="1"/>
0350	<ProtocolVersionMinor type="Integer" value="1"/>
0351	</ProtocolVersion>
0352	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0353	<BatchCount type="Integer" value="1"/>
0354	</ResponseHeader>
0355	<BatchItem>
0356	<Operation type="Enumeration" value="Revoke"/>
0357	<ResultStatus type="Enumeration" value="Success"/>
0358	<ResponsePayload>
0359	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0360	</ResponsePayload>
0361	</BatchItem>
0362	</ResponseMessage>
	# TIME 8
0363	<RequestMessage>
0364	<RequestHeader>
0365	<ProtocolVersion>
0366	<ProtocolVersionMajor type="Integer" value="1"/>
0367	<ProtocolVersionMinor type="Integer" value="1"/>
0368	</ProtocolVersion>
0369	<BatchCount type="Integer" value="1"/>
0370	</RequestHeader>
0371	<BatchItem>
0372	<Operation type="Enumeration" value="GetAttributes"/>
0373	<RequestPayload>
0374	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0375	<AttributeName type="TextString" value="State"/>
0376	</RequestPayload>
0377	</BatchItem>
0378	</RequestMessage>
0379	<ResponseMessage>
0380	<ResponseHeader>
0381	<ProtocolVersion>
0382	<ProtocolVersionMajor type="Integer" value="1"/>
0383	<ProtocolVersionMinor type="Integer" value="1"/>
0384	</ProtocolVersion>
0385	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0386	<BatchCount type="Integer" value="1"/>
0387	</ResponseHeader>
0388	<BatchItem>
0389	<Operation type="Enumeration" value="GetAttributes"/>
0390	<ResultStatus type="Enumeration" value="Success"/>
0391	<ResponsePayload>
0392	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0393	<Attribute>
0394	<AttributeName type="TextString" value="State"/>
0395	<AttributeValue type="Enumeration" value="Compromised"/>
0396	</Attribute>
0397	</ResponsePayload>
0398	</BatchItem>
0399	</ResponseMessage>
	# TIME 9

```

0400 <RequestMessage>
0401   <RequestHeader>
0402     <ProtocolVersion>
0403       <ProtocolVersionMajor type="Integer" value="1"/>
0404       <ProtocolVersionMinor type="Integer" value="1"/>
0405     </ProtocolVersion>
0406     <BatchCount type="Integer" value="1"/>
0407   </RequestHeader>
0408   <BatchItem>
0409     <Operation type="Enumeration" value="Destroy"/>
0410     <RequestPayload>
0411       <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0412     </RequestPayload>
0413   </BatchItem>
0414 </RequestMessage>
0415 <ResponseMessage>
0416   <ResponseHeader>
0417     <ProtocolVersion>
0418       <ProtocolVersionMajor type="Integer" value="1"/>
0419       <ProtocolVersionMinor type="Integer" value="1"/>
0420     </ProtocolVersion>
0421     <TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0422     <BatchCount type="Integer" value="1"/>
0423   </ResponseHeader>
0424   <BatchItem>
0425     <Operation type="Enumeration" value="Destroy"/>
0426     <ResultStatus type="Enumeration" value="Success"/>
0427     <ResponsePayload>
0428       <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0429     </ResponsePayload>
0430   </BatchItem>
0431 </ResponseMessage>

```

117

### 118 3.2.3 AKLC-M-3-11

119 CreateKeyPair, 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="CreateKeyPair"/>
0011     <RequestPayload>
0012       <CommonTemplateAttribute>
0013         <Attribute>
0014           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0015           <AttributeValue type="Enumeration" value="RSA"/>
0016         </Attribute>

```

```

0017         <Attribute>
0018         <AttributeName type="TextString" value="Cryptographic
Length"/>
0019         <AttributeValue type="Integer" value="2048"/>
0020         </Attribute>
0021     </CommonTemplateAttribute>
0022     <PrivateKeyTemplateAttribute>
0023     <Attribute>
0024     <AttributeName type="TextString" value="Name"/>
0025     <AttributeValue>
0026     <NameValue type="TextString" value="AKLC-M-3-11-
private"/>
0027     <NameType type="Enumeration"
value="UninterpretedTextString"/>
0028     </AttributeValue>
0029     </Attribute>
0030     <Attribute>
0031     <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0032     <AttributeValue type="Integer" value="Sign"/>
0033     </Attribute>
0034     </PrivateKeyTemplateAttribute>
0035     <PublicKeyTemplateAttribute>
0036     <Attribute>
0037     <AttributeName type="TextString" value="Name"/>
0038     <AttributeValue>
0039     <NameValue type="TextString" value="AKLC-M-3-11-
public"/>
0040     <NameType type="Enumeration"
value="UninterpretedTextString"/>
0041     </AttributeValue>
0042     </Attribute>
0043     <Attribute>
0044     <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0045     <AttributeValue type="Integer" value="Verify"/>
0046     </Attribute>
0047     </PublicKeyTemplateAttribute>
0048     </RequestPayload>
0049     </BatchItem>
0050 </RequestMessage>
0051 <ResponseMessage>
0052 <ResponseHeader>
0053 <ProtocolVersion>
0054 <ProtocolVersionMajor type="Integer" value="1"/>
0055 <ProtocolVersionMinor type="Integer" value="1"/>
0056 </ProtocolVersion>
0057 <TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/>
0058 <BatchCount type="Integer" value="1"/>
0059 </ResponseHeader>
0060 <BatchItem>
0061 <Operation type="Enumeration" value="CreateKeyPair"/>
0062 <ResultStatus type="Enumeration" value="Success"/>
0063 <ResponsePayload>
0064 <PrivateKeyUniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0065 <PublicKeyUniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>

```

0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
0069	# TIME 1 <RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="1"/>
0074	</ProtocolVersion>
0075	<BatchCount type="Integer" value="1"/>
0076	</RequestHeader>
0077	<BatchItem>
0078	<Operation type="Enumeration" value="GetAttributes"/>
0079	<RequestPayload>
0080	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0081	<AttributeName type="TextString" value="State"/>
0082	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0083	<AttributeName type="TextString" value="Unique Identifier"/>
0084	<AttributeName type="TextString" value="Object Type"/>
0085	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0086	<AttributeName type="TextString" value="Cryptographic Length"/>
0087	<AttributeName type="TextString" value="Digest"/>
0088	<AttributeName type="TextString" value="Initial Date"/>
0089	<AttributeName type="TextString" value="Last Change Date"/>
0090	</RequestPayload>
0091	</BatchItem>
0092	</RequestMessage>
0093	<ResponseMessage>
0094	<ResponseHeader>
0095	<ProtocolVersion>
0096	<ProtocolVersionMajor type="Integer" value="1"/>
0097	<ProtocolVersionMinor type="Integer" value="1"/>
0098	</ProtocolVersion>
0099	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0100	<BatchCount type="Integer" value="1"/>
0101	</ResponseHeader>
0102	<BatchItem>
0103	<Operation type="Enumeration" value="GetAttributes"/>
0104	<ResultStatus type="Enumeration" value="Success"/>
0105	<ResponsePayload>
0106	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0107	<Attribute>
0108	<AttributeName type="TextString" value="State"/>
0109	<AttributeValue type="Enumeration" value="PreActive"/>
0110	</Attribute>
0111	<Attribute>
0112	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0113	<AttributeValue type="Integer" value="Sign"/>
0114	</Attribute>
0115	<Attribute>
0116	<AttributeName type="TextString" value="Unique Identifier"/>

0117	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0118	</Attribute>
0119	<Attribute>
0120	<AttributeName type="TextString" value="Object Type"/>
0121	<AttributeValue type="Enumeration" value="PrivateKey"/>
0122	</Attribute>
0123	<Attribute>
0124	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0125	<AttributeValue type="Enumeration" value="RSA"/>
0126	</Attribute>
0127	<Attribute>
0128	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0129	<AttributeValue type="Integer" value="2048"/>
0130	</Attribute>
0131	<Attribute>
0132	<AttributeName type="TextString" value="Digest"/>
0133	<AttributeValue>
0134	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0135	<DigestValue type="ByteString"
	value="8eb422ae2b006a05d3c8a542a28536735241b6dc1c37926bc8007bd6220d9
	230"/>
0136	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0137	</AttributeValue>
0138	</Attribute>
0139	<Attribute>
0140	<AttributeName type="TextString" value="Initial Date"/>
0141	<AttributeValue type="DateTime" value="2013-01-
	11T08:18:21+00:00"/>
0142	</Attribute>
0143	<Attribute>
0144	<AttributeName type="TextString" value="Last Change Date"/>
0145	<AttributeValue type="DateTime" value="2013-01-
	11T08:18:21+00:00"/>
0146	</Attribute>
0147	</ResponsePayload>
0148	</BatchItem>
0149	</ResponseMessage>
	# TIME 2
0150	<RequestMessage>
0151	<RequestHeader>
0152	<ProtocolVersion>
0153	<ProtocolVersionMajor type="Integer" value="1"/>
0154	<ProtocolVersionMinor type="Integer" value="1"/>
0155	</ProtocolVersion>
0156	<BatchCount type="Integer" value="1"/>
0157	</RequestHeader>
0158	<BatchItem>
0159	<Operation type="Enumeration" value="Activate"/>
0160	<RequestPayload>
0161	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0162	</RequestPayload>
0163	</BatchItem>
0164	</RequestMessage>
0165	<ResponseMessage>



0166	<ResponseHeader>
0167	<ProtocolVersion>
0168	<ProtocolVersionMajor type="Integer" value="1"/>
0169	<ProtocolVersionMinor type="Integer" value="1"/>
0170	</ProtocolVersion>
0171	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0172	<BatchCount type="Integer" value="1"/>
0173	</ResponseHeader>
0174	<BatchItem>
0175	<Operation type="Enumeration" value="Activate"/>
0176	<ResultStatus type="Enumeration" value="Success"/>
0177	<ResponsePayload>
0178	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0179	</ResponsePayload>
0180	</BatchItem>
0181	</ResponseMessage>
	# TIME 3
0182	<RequestMessage>
0183	<RequestHeader>
0184	<ProtocolVersion>
0185	<ProtocolVersionMajor type="Integer" value="1"/>
0186	<ProtocolVersionMinor type="Integer" value="1"/>
0187	</ProtocolVersion>
0188	<BatchCount type="Integer" value="1"/>
0189	</RequestHeader>
0190	<BatchItem>
0191	<Operation type="Enumeration" value="GetAttributes"/>
0192	<RequestPayload>
0193	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0194	<AttributeName type="TextString" value="State"/>
0195	<AttributeName type="TextString" value="Activation Date"/>
0196	<AttributeName type="TextString" value="Deactivation Date"/>
0197	</RequestPayload>
0198	</BatchItem>
0199	</RequestMessage>
0200	<ResponseMessage>
0201	<ResponseHeader>
0202	<ProtocolVersion>
0203	<ProtocolVersionMajor type="Integer" value="1"/>
0204	<ProtocolVersionMinor type="Integer" value="1"/>
0205	</ProtocolVersion>
0206	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0207	<BatchCount type="Integer" value="1"/>
0208	</ResponseHeader>
0209	<BatchItem>
0210	<Operation type="Enumeration" value="GetAttributes"/>
0211	<ResultStatus type="Enumeration" value="Success"/>
0212	<ResponsePayload>
0213	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0214	<Attribute>
0215	<AttributeName type="TextString" value="State"/>
0216	<AttributeValue type="Enumeration" value="Active"/>
0217	</Attribute>
0218	<Attribute>
0219	<AttributeName type="TextString" value="Activation Date"/>

0220	<AttributeValue type="DateTime" value="2013-01-10T23:36:01+00:00"/>
0221	</Attribute>
0222	</ResponsePayload>
0223	</BatchItem>
0224	</ResponseMessage>
0225	# TIME 4 <RequestMessage>
0226	<RequestHeader>
0227	<ProtocolVersion>
0228	<ProtocolVersionMajor type="Integer" value="1"/>
0229	<ProtocolVersionMinor type="Integer" value="1"/>
0230	</ProtocolVersion>
0231	<BatchCount type="Integer" value="1"/>
0232	</RequestHeader>
0233	<BatchItem>
0234	<Operation type="Enumeration" value="ModifyAttribute"/>
0235	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0236	<RequestPayload>
0237	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0238	<Attribute>
0239	<AttributeName type="TextString" value="Activation Date"/>
0240	<AttributeValue type="DateTime" value="\$NOW"/>
0241	</Attribute>
0242	</RequestPayload>
0243	</BatchItem>
0244	</RequestMessage>
0245	<ResponseMessage>
0246	<ResponseHeader>
0247	<ProtocolVersion>
0248	<ProtocolVersionMajor type="Integer" value="1"/>
0249	<ProtocolVersionMinor type="Integer" value="1"/>
0250	</ProtocolVersion>
0251	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0252	<BatchCount type="Integer" value="1"/>
0253	</ResponseHeader>
0254	<BatchItem>
0255	<Operation type="Enumeration" value="ModifyAttribute"/>
0256	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0257	<ResultStatus type="Enumeration" value="OperationFailed"/>
0258	<ResultReason type="Enumeration" value="PermissionDenied"/>
0259	<ResultMessage type="TextString" value="DENIED"/>
0260	</BatchItem>
0261	</ResponseMessage>
0262	# TIME 5 <RequestMessage>
0263	<RequestHeader>
0264	<ProtocolVersion>
0265	<ProtocolVersionMajor type="Integer" value="1"/>
0266	<ProtocolVersionMinor type="Integer" value="1"/>
0267	</ProtocolVersion>
0268	<BatchCount type="Integer" value="1"/>
0269	</RequestHeader>
0270	<BatchItem>
0271	<Operation type="Enumeration" value="Revoke"/>
0272	<RequestPayload>
0273	<UniqueIdentifier type="TextString"

0274	value="\$UNIQUE_IDENTIFIER_0"/>
0275	<RevocationReason>
0276	<RevocationReasonCode type="Enumeration"
0277	value="KeyCompromise"/>
0278	</RevocationReason>
0279	<CompromiseOccurrenceDate type="DateTime" value="1970-01-01T00:00:06+00:00"/>
0280	</RequestPayload>
0281	</BatchItem>
0282	</RequestMessage>
0283	<ResponseMessage>
0284	<ResponseHeader>
0285	<ProtocolVersion>
0286	<ProtocolVersionMajor type="Integer" value="1"/>
0287	<ProtocolVersionMinor type="Integer" value="1"/>
0288	</ProtocolVersion>
0289	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0290	<BatchCount type="Integer" value="1"/>
0291	</ResponseHeader>
0292	<BatchItem>
0293	<Operation type="Enumeration" value="Revoke"/>
0294	<ResultStatus type="Enumeration" value="Success"/>
0295	<ResponsePayload>
0296	<UniqueIdentifier type="TextString"
0297	value="\$UNIQUE_IDENTIFIER_0"/>
0298	</ResponsePayload>
0299	</BatchItem>
0300	</ResponseMessage>
0301	# TIME 6
0302	<RequestMessage>
0303	<RequestHeader>
0304	<ProtocolVersion>
0305	<ProtocolVersionMajor type="Integer" value="1"/>
0306	<ProtocolVersionMinor type="Integer" value="1"/>
0307	</ProtocolVersion>
0308	<BatchCount type="Integer" value="1"/>
0309	</RequestHeader>
0310	<BatchItem>
0311	<Operation type="Enumeration" value="GetAttributes"/>
0312	<RequestPayload>
0313	<UniqueIdentifier type="TextString"
0314	value="\$UNIQUE_IDENTIFIER_0"/>
0315	<AttributeName type="TextString" value="State"/>
0316	</RequestPayload>
0317	</BatchItem>
0318	</RequestMessage>
0319	<ResponseMessage>
0320	<ResponseHeader>
0321	<ProtocolVersion>
0322	<ProtocolVersionMajor type="Integer" value="1"/>
0323	<ProtocolVersionMinor type="Integer" value="1"/>
0324	</ProtocolVersion>
0325	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
	<BatchCount type="Integer" value="1"/>
	</ResponseHeader>
	<BatchItem>
	<Operation type="Enumeration" value="GetAttributes"/>
	<ResultStatus type="Enumeration" value="Success"/>

0326	<ResponsePayload>
0327	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0328	<Attribute>
0329	<AttributeName type="TextString" value="State"/>
0330	<AttributeValue type="Enumeration" value="Compromised"/>
0331	</Attribute>
0332	</ResponsePayload>
0333	</BatchItem>
0334	</ResponseMessage>
	# TIME 7
0335	<RequestMessage>
0336	<RequestHeader>
0337	<ProtocolVersion>
0338	<ProtocolVersionMajor type="Integer" value="1"/>
0339	<ProtocolVersionMinor type="Integer" value="1"/>
0340	</ProtocolVersion>
0341	<BatchCount type="Integer" value="1"/>
0342	</RequestHeader>
0343	<BatchItem>
0344	<Operation type="Enumeration" value="GetAttributes"/>
0345	<RequestPayload>
0346	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0347	<AttributeName type="TextString" value="State"/>
0348	</RequestPayload>
0349	</BatchItem>
0350	</RequestMessage>
0351	<ResponseMessage>
0352	<ResponseHeader>
0353	<ProtocolVersion>
0354	<ProtocolVersionMajor type="Integer" value="1"/>
0355	<ProtocolVersionMinor type="Integer" value="1"/>
0356	</ProtocolVersion>
0357	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0358	<BatchCount type="Integer" value="1"/>
0359	</ResponseHeader>
0360	<BatchItem>
0361	<Operation type="Enumeration" value="GetAttributes"/>
0362	<ResultStatus type="Enumeration" value="Success"/>
0363	<ResponsePayload>
0364	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0365	<Attribute>
0366	<AttributeName type="TextString" value="State"/>
0367	<AttributeValue type="Enumeration" value="PreActive"/>
0368	</Attribute>
0369	</ResponsePayload>
0370	</BatchItem>
0371	</ResponseMessage>
	# TIME 8
0372	<RequestMessage>
0373	<RequestHeader>
0374	<ProtocolVersion>
0375	<ProtocolVersionMajor type="Integer" value="1"/>
0376	<ProtocolVersionMinor type="Integer" value="1"/>
0377	</ProtocolVersion>
0378	<BatchCount type="Integer" value="1"/>

0379	</RequestHeader>
0380	<BatchItem>
0381	<Operation type="Enumeration" value="Destroy"/>
0382	<RequestPayload>
0383	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0384	</RequestPayload>
0385	</BatchItem>
0386	</RequestMessage>
0387	<ResponseMessage>
0388	<ResponseHeader>
0389	<ProtocolVersion>
0390	<ProtocolVersionMajor type="Integer" value="1"/>
0391	<ProtocolVersionMinor type="Integer" value="1"/>
0392	</ProtocolVersion>
0393	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0394	<BatchCount type="Integer" value="1"/>
0395	</ResponseHeader>
0396	<BatchItem>
0397	<Operation type="Enumeration" value="Destroy"/>
0398	<ResultStatus type="Enumeration" value="Success"/>
0399	<ResponsePayload>
0400	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0401	</ResponsePayload>
0402	</BatchItem>
0403	</ResponseMessage>
0404	# TIME 9 <RequestMessage>
0405	<RequestHeader>
0406	<ProtocolVersion>
0407	<ProtocolVersionMajor type="Integer" value="1"/>
0408	<ProtocolVersionMinor type="Integer" value="1"/>
0409	</ProtocolVersion>
0410	<BatchCount type="Integer" value="1"/>
0411	</RequestHeader>
0412	<BatchItem>
0413	<Operation type="Enumeration" value="Destroy"/>
0414	<RequestPayload>
0415	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0416	</RequestPayload>
0417	</BatchItem>
0418	</RequestMessage>
0419	<ResponseMessage>
0420	<ResponseHeader>
0421	<ProtocolVersion>
0422	<ProtocolVersionMajor type="Integer" value="1"/>
0423	<ProtocolVersionMinor type="Integer" value="1"/>
0424	</ProtocolVersion>
0425	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0426	<BatchCount type="Integer" value="1"/>
0427	</ResponseHeader>
0428	<BatchItem>
0429	<Operation type="Enumeration" value="Destroy"/>
0430	<ResultStatus type="Enumeration" value="Success"/>
0431	<ResponsePayload>
0432	<UniqueIdentifier type="TextString"

0433	value="\$UNIQUE_IDENTIFIER_1"/>
0434	</ResponsePayload>
0435	</BatchItem>
	</ResponseMessage>

120

## 121 3.3 Mandatory Test Cases KMIP v1.2

### 122 3.3.1 AKLC-M-1-12

#### 123 CreateKeyPair, GetAttributes, 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>
0008     <BatchCount type="Integer" value="1"/>
0009   </RequestHeader>
0010   <BatchItem>
0011     <Operation type="Enumeration" value="CreateKeyPair"/>
0012     <RequestPayload>
0013       <CommonTemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
0016           Algorithm"/>
0017           <AttributeValue type="Enumeration" value="RSA"/>
0018         </Attribute>
0019         <AttributeName type="TextString" value="Cryptographic
0020         Length"/>
0021         <AttributeValue type="Integer" value="2048"/>
0022       </CommonTemplateAttribute>
0023       <PrivateKeyTemplateAttribute>
0024         <Attribute>
0025           <AttributeName type="TextString" value="Name"/>
0026           <AttributeValue>
0027             <NameValue type="TextString" value="AKLC-M-1-12-
0028             private"/>
0029             <NameType type="Enumeration"
0030             value="UninterpretedTextString"/>
0031           </AttributeValue>
0032         </Attribute>
0033         <AttributeName type="TextString" value="Cryptographic
0034         Usage Mask"/>
0035         <AttributeValue type="Integer" value="Sign"/>
0036       </PrivateKeyTemplateAttribute>
0037       <PublicKeyTemplateAttribute>
0038         <Attribute>
0039           <AttributeName type="TextString" value="Name"/>
0040           <AttributeValue>
0041             <NameValue type="TextString" value="AKLC-M-1-12-
0042             public"/>

```

0040	<pre>                 &lt;NameType type="Enumeration" value="UninterpretedTextString"/&gt; 0041                &lt;/AttributeValue&gt; 0042                &lt;/Attribute&gt; 0043                &lt;Attribute&gt; 0044                &lt;AttributeName type="TextString" value="Cryptographic Usage Mask"/&gt; 0045                &lt;AttributeValue type="Integer" value="Verify"/&gt; 0046                &lt;/Attribute&gt; 0047                &lt;/PublicKeyTemplateAttribute&gt; 0048                &lt;/RequestPayload&gt; 0049                &lt;/BatchItem&gt; 0050            &lt;/RequestMessage&gt; </pre>
0051	<pre> &lt;ResponseMessage&gt; 0052     &lt;ResponseHeader&gt; 0053         &lt;ProtocolVersion&gt; 0054             &lt;ProtocolVersionMajor type="Integer" value="1"/&gt; 0055             &lt;ProtocolVersionMinor type="Integer" value="2"/&gt; 0056         &lt;/ProtocolVersion&gt; 0057         &lt;TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/&gt; 0058         &lt;BatchCount type="Integer" value="1"/&gt; 0059     &lt;/ResponseHeader&gt; 0060     &lt;BatchItem&gt; 0061         &lt;Operation type="Enumeration" value="CreateKeyPair"/&gt; 0062         &lt;ResultStatus type="Enumeration" value="Success"/&gt; 0063         &lt;ResponsePayload&gt; 0064             &lt;PrivateKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/&gt; 0065             &lt;PublicKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/&gt; 0066         &lt;/ResponsePayload&gt; 0067     &lt;/BatchItem&gt; 0068 &lt;/ResponseMessage&gt; </pre>
0069	<pre> # TIME 1 &lt;RequestMessage&gt; 0070     &lt;RequestHeader&gt; 0071         &lt;ProtocolVersion&gt; 0072             &lt;ProtocolVersionMajor type="Integer" value="1"/&gt; 0073             &lt;ProtocolVersionMinor type="Integer" value="2"/&gt; 0074         &lt;/ProtocolVersion&gt; 0075         &lt;BatchCount type="Integer" value="1"/&gt; 0076     &lt;/RequestHeader&gt; 0077     &lt;BatchItem&gt; 0078         &lt;Operation type="Enumeration" value="GetAttributes"/&gt; 0079         &lt;RequestPayload&gt; 0080             &lt;UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/&gt; 0081             &lt;AttributeName type="TextString" value="State"/&gt; 0082             &lt;AttributeName type="TextString" value="Cryptographic Usage Mask"/&gt; 0083             &lt;AttributeName type="TextString" value="Unique Identifier"/&gt; 0084             &lt;AttributeName type="TextString" value="Object Type"/&gt; 0085             &lt;AttributeName type="TextString" value="Cryptographic Algorithm"/&gt; 0086             &lt;AttributeName type="TextString" value="Cryptographic Length"/&gt; 0087             &lt;AttributeName type="TextString" value="Digest"/&gt; 0088             &lt;AttributeName type="TextString" value="Initial Date"/&gt; </pre>

0089	<AttributeName type="TextString" value="Last Change Date"/>
0090	<AttributeName type="TextString" value="Activation Date"/>
0091	<AttributeName type="TextString" value="Original Creation Date"/>
0092	</RequestPayload>
0093	</BatchItem>
0094	</RequestMessage>
0095	<ResponseMessage>
0096	<ResponseHeader>
0097	<ProtocolVersion>
0098	<ProtocolVersionMajor type="Integer" value="1"/>
0099	<ProtocolVersionMinor type="Integer" value="2"/>
0100	</ProtocolVersion>
0101	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0102	<BatchCount type="Integer" value="1"/>
0103	</ResponseHeader>
0104	<BatchItem>
0105	<Operation type="Enumeration" value="GetAttributes"/>
0106	<ResultStatus type="Enumeration" value="Success"/>
0107	<ResponsePayload>
0108	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0109	<Attribute>
0110	<AttributeName type="TextString" value="State"/>
0111	<AttributeValue type="Enumeration" value="PreActive"/>
0112	</Attribute>
0113	<Attribute>
0114	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0115	<AttributeValue type="Integer" value="Sign"/>
0116	</Attribute>
0117	<Attribute>
0118	<AttributeName type="TextString" value="Unique Identifier"/>
0119	<AttributeValue type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0120	</Attribute>
0121	<Attribute>
0122	<AttributeName type="TextString" value="Object Type"/>
0123	<AttributeValue type="Enumeration" value="PrivateKey"/>
0124	</Attribute>
0125	<Attribute>
0126	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0127	<AttributeValue type="Enumeration" value="RSA"/>
0128	</Attribute>
0129	<Attribute>
0130	<AttributeName type="TextString" value="Cryptographic Length"/>
0131	<AttributeValue type="Integer" value="2048"/>
0132	</Attribute>
0133	<Attribute>
0134	<AttributeName type="TextString" value="Digest"/>
0135	<AttributeValue>
0136	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0137	<DigestValue type="ByteString" value="8eb422ae2b006a05d3c8a542a28536735241b6dc1c37926bc8007bd6220d9 230"/>
0138	<KeyFormatType type="Enumeration" value="PKCS 1"/>



0139	</AttributeValue>
0140	</Attribute>
0141	<Attribute>
0142	<AttributeName type="TextString" value="Initial Date"/>
0143	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0144	</Attribute>
0145	<Attribute>
0146	<AttributeName type="TextString" value="Last Change Date"/>
0147	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0148	</Attribute>
0149	<Attribute>
0150	<AttributeName type="TextString" value="Original Creation Date"/>
0151	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0152	</Attribute>
0153	</ResponsePayload>
0154	</BatchItem>
0155	</ResponseMessage>
0156	# TIME 2 <RequestMessage>
0157	<RequestHeader>
0158	<ProtocolVersion>
0159	<ProtocolVersionMajor type="Integer" value="1"/>
0160	<ProtocolVersionMinor type="Integer" value="2"/>
0161	</ProtocolVersion>
0162	<BatchCount type="Integer" value="1"/>
0163	</RequestHeader>
0164	<BatchItem>
0165	<Operation type="Enumeration" value="GetAttributes"/>
0166	<RequestPayload>
0167	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0168	<AttributeName type="TextString" value="State"/>
0169	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0170	<AttributeName type="TextString" value="Unique Identifier"/>
0171	<AttributeName type="TextString" value="Object Type"/>
0172	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0173	<AttributeName type="TextString" value="Cryptographic Length"/>
0174	<AttributeName type="TextString" value="Digest"/>
0175	<AttributeName type="TextString" value="Initial Date"/>
0176	<AttributeName type="TextString" value="Last Change Date"/>
0177	<AttributeName type="TextString" value="Activation Date"/>
0178	<AttributeName type="TextString" value="Original Creation Date"/>
0179	</RequestPayload>
0180	</BatchItem>
0181	</RequestMessage>
0182	<ResponseMessage>
0183	<ResponseHeader>
0184	<ProtocolVersion>
0185	<ProtocolVersionMajor type="Integer" value="1"/>
0186	<ProtocolVersionMinor type="Integer" value="2"/>

```

0187     </ProtocolVersion>
0188     <TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0189     <BatchCount type="Integer" value="1"/>
0190 </ResponseHeader>
0191 <BatchItem>
0192     <Operation type="Enumeration" value="GetAttributes"/>
0193     <ResultStatus type="Enumeration" value="Success"/>
0194     <ResponsePayload>
0195         <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0196         <Attribute>
0197             <AttributeName type="TextString" value="State"/>
0198             <AttributeValue type="Enumeration" value="PreActive"/>
0199         </Attribute>
0200         <Attribute>
0201             <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0202             <AttributeValue type="Integer" value="Verify"/>
0203         </Attribute>
0204         <Attribute>
0205             <AttributeName type="TextString" value="Unique Identifier"/>
0206             <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0207         </Attribute>
0208         <Attribute>
0209             <AttributeName type="TextString" value="Object Type"/>
0210             <AttributeValue type="Enumeration" value="PublicKey"/>
0211         </Attribute>
0212         <Attribute>
0213             <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0214             <AttributeValue type="Enumeration" value="RSA"/>
0215         </Attribute>
0216         <Attribute>
0217             <AttributeName type="TextString" value="Cryptographic
Length"/>
0218             <AttributeValue type="Integer" value="2048"/>
0219         </Attribute>
0220         <Attribute>
0221             <AttributeName type="TextString" value="Digest"/>
0222             <AttributeValue>
0223                 <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0224                 <DigestValue type="ByteString"
value="82bcff8afab753809db804e654013ded708c3996a50c6ce9313f9b3915442
ce9"/>
0225             <KeyFormatType type="Enumeration" value="PKCS_1"/>
0226         </AttributeValue>
0227         </Attribute>
0228         <Attribute>
0229             <AttributeName type="TextString" value="Initial Date"/>
0230             <AttributeValue type="DateTime" value="2013-01-
11T08:19:49+00:00"/>
0231         </Attribute>
0232         <Attribute>
0233             <AttributeName type="TextString" value="Last Change Date"/>
0234             <AttributeValue type="DateTime" value="2013-01-
11T08:19:49+00:00"/>
0235         </Attribute>

```

0236	<Attribute>
0237	<AttributeName type="TextString" value="Original Creation Date"/>
0238	<AttributeValue type="DateTime" value="2013-01-11T08:19:49+00:00"/>
0239	</Attribute>
0240	</ResponsePayload>
0241	</BatchItem>
0242	</ResponseMessage>
# TIME 3	
0243	<RequestMessage>
0244	<RequestHeader>
0245	<ProtocolVersion>
0246	<ProtocolVersionMajor type="Integer" value="1"/>
0247	<ProtocolVersionMinor type="Integer" value="2"/>
0248	</ProtocolVersion>
0249	<BatchCount type="Integer" value="1"/>
0250	</RequestHeader>
0251	<BatchItem>
0252	<Operation type="Enumeration" value="Destroy"/>
0253	<RequestPayload>
0254	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0255	</RequestPayload>
0256	</BatchItem>
0257	</RequestMessage>
# TIME 4	
0258	<ResponseMessage>
0259	<ResponseHeader>
0260	<ProtocolVersion>
0261	<ProtocolVersionMajor type="Integer" value="1"/>
0262	<ProtocolVersionMinor type="Integer" value="2"/>
0263	</ProtocolVersion>
0264	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0265	<BatchCount type="Integer" value="1"/>
0266	</ResponseHeader>
0267	<BatchItem>
0268	<Operation type="Enumeration" value="Destroy"/>
0269	<ResultStatus type="Enumeration" value="Success"/>
0270	<ResponsePayload>
0271	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0272	</ResponsePayload>
0273	</BatchItem>
0274	</ResponseMessage>
# TIME 4	
0275	<RequestMessage>
0276	<RequestHeader>
0277	<ProtocolVersion>
0278	<ProtocolVersionMajor type="Integer" value="1"/>
0279	<ProtocolVersionMinor type="Integer" value="2"/>
0280	</ProtocolVersion>
0281	<BatchCount type="Integer" value="1"/>
0282	</RequestHeader>
0283	<BatchItem>
0284	<Operation type="Enumeration" value="Destroy"/>
0285	<RequestPayload>
0286	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>

0287	</RequestPayload>
0288	</BatchItem>
0289	</RequestMessage>
0290	<ResponseMessage>
0291	<ResponseHeader>
0292	<ProtocolVersion>
0293	<ProtocolVersionMajor type="Integer" value="1"/>
0294	<ProtocolVersionMinor type="Integer" value="2"/>
0295	</ProtocolVersion>
0296	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0297	<BatchCount type="Integer" value="1"/>
0298	</ResponseHeader>
0299	<BatchItem>
0300	<Operation type="Enumeration" value="Destroy"/>
0301	<ResultStatus type="Enumeration" value="Success"/>
0302	<ResponsePayload>
0303	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0304	</ResponsePayload>
0305	</BatchItem>
0306	</ResponseMessage>

124

### 125 3.3.2 AKLC-M-2-12

126 CreateKeyPair, 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="CreateKeyPair"/>
0011	<RequestPayload>
0012	<CommonTemplateAttribute>
0013	<Attribute>
0014	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0015	<AttributeValue type="Enumeration" value="RSA"/>
0016	</Attribute>
0017	<Attribute>
0018	<AttributeName type="TextString" value="Cryptographic Length"/>
0019	<AttributeValue type="Integer" value="2048"/>
0020	</Attribute>
0021	</CommonTemplateAttribute>
0022	<PrivateKeyTemplateAttribute>
0023	<Attribute>
0024	<AttributeName type="TextString" value="Name"/>
0025	<AttributeValue>
0026	<NameValue type="TextString" value="AKLC-M-2-12-private"/>
0027	<NameType type="Enumeration"

0028	value="UninterpretedTextString"/>
0029	</AttributeValue>
0030	</Attribute>
0031	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0032	<AttributeValue type="Integer" value="Sign"/>
0033	</Attribute>
0034	</PrivateKeyTemplateAttribute>
0035	<PublicKeyTemplateAttribute>
0036	<Attribute>
0037	<AttributeName type="TextString" value="Name"/>
0038	<AttributeValue>
0039	<NameValue type="TextString" value="AKLC-M-2-12-public"/>
0040	<NameType type="Enumeration" value="UninterpretedTextString"/>
0041	</AttributeValue>
0042	</Attribute>
0043	<Attribute>
0044	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0045	<AttributeValue type="Integer" value="Verify"/>
0046	</Attribute>
0047	</PublicKeyTemplateAttribute>
0048	</RequestPayload>
0049	</BatchItem>
0050	</RequestMessage>
0051	<ResponseMessage>
0052	<ResponseHeader>
0053	<ProtocolVersion>
0054	<ProtocolVersionMajor type="Integer" value="1"/>
0055	<ProtocolVersionMinor type="Integer" value="2"/>
0056	</ProtocolVersion>
0057	<TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/>
0058	<BatchCount type="Integer" value="1"/>
0059	</ResponseHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="CreateKeyPair"/>
0062	<ResultStatus type="Enumeration" value="Success"/>
0063	<ResponsePayload>
0064	<PrivateKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0065	<PublicKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
0069	# TIME 1 <RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="2"/>
0074	</ProtocolVersion>
0075	<BatchCount type="Integer" value="1"/>
0076	</RequestHeader>
0077	<BatchItem>

```

0078     <Operation type="Enumeration" value="GetAttributes"/>
0079     <RequestPayload>
0080         <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0081         <AttributeName type="TextString" value="State"/>
0082         <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0083         <AttributeName type="TextString" value="Unique Identifier"/>
0084         <AttributeName type="TextString" value="Object Type"/>
0085         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0086         <AttributeName type="TextString" value="Cryptographic
Length"/>
0087         <AttributeName type="TextString" value="Digest"/>
0088         <AttributeName type="TextString" value="Initial Date"/>
0089         <AttributeName type="TextString" value="Last Change Date"/>
0090         <AttributeName type="TextString" value="Original Creation
Date"/>
0091     </RequestPayload>
0092 </BatchItem>
0093 </RequestMessage>
0094 <ResponseMessage>
0095     <ResponseHeader>
0096         <ProtocolVersion>
0097             <ProtocolVersionMajor type="Integer" value="1"/>
0098             <ProtocolVersionMinor type="Integer" value="2"/>
0099         </ProtocolVersion>
0100         <TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0101         <BatchCount type="Integer" value="1"/>
0102     </ResponseHeader>
0103     <BatchItem>
0104         <Operation type="Enumeration" value="GetAttributes"/>
0105         <ResultStatus type="Enumeration" value="Success"/>
0106         <ResponsePayload>
0107             <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0108             <Attribute>
0109                 <AttributeName type="TextString" value="State"/>
0110                 <AttributeValue type="Enumeration" value="PreActive"/>
0111             </Attribute>
0112             <Attribute>
0113                 <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0114                 <AttributeValue type="Integer" value="Sign"/>
0115             </Attribute>
0116             <Attribute>
0117                 <AttributeName type="TextString" value="Unique Identifier"/>
0118                 <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0119             </Attribute>
0120             <Attribute>
0121                 <AttributeName type="TextString" value="Object Type"/>
0122                 <AttributeValue type="Enumeration" value="PrivateKey"/>
0123             </Attribute>
0124             <Attribute>
0125                 <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0126                 <AttributeValue type="Enumeration" value="RSA"/>

```

0127	</Attribute>
0128	<Attribute>
0129	<AttributeName type="TextString" value="Cryptographic Length"/>
0130	<AttributeValue type="Integer" value="2048"/>
0131	</Attribute>
0132	<Attribute>
0133	<AttributeName type="TextString" value="Digest"/>
0134	<AttributeValue>
0135	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0136	<DigestValue type="ByteString" value="8eb422ae2b006a05d3c8a542a28536735241b6dc1c37926bc8007bd6220d9230"/>
0137	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0138	</AttributeValue>
0139	</Attribute>
0140	<Attribute>
0141	<AttributeName type="TextString" value="Initial Date"/>
0142	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0143	</Attribute>
0144	<Attribute>
0145	<AttributeName type="TextString" value="Last Change Date"/>
0146	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0147	</Attribute>
0148	<Attribute>
0149	<AttributeName type="TextString" value="Original Creation Date"/>
0150	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0151	</Attribute>
0152	</ResponsePayload>
0153	</BatchItem>
0154	</ResponseMessage>
0155	# TIME 2 <RequestMessage>
0156	<RequestHeader>
0157	<ProtocolVersion>
0158	<ProtocolVersionMajor type="Integer" value="1"/>
0159	<ProtocolVersionMinor type="Integer" value="2"/>
0160	</ProtocolVersion>
0161	<BatchCount type="Integer" value="1"/>
0162	</RequestHeader>
0163	<BatchItem>
0164	<Operation type="Enumeration" value="Activate"/>
0165	<RequestPayload>
0166	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0167	</RequestPayload>
0168	</BatchItem>
0169	</RequestMessage>
0170	<ResponseMessage>
0171	<ResponseHeader>
0172	<ProtocolVersion>
0173	<ProtocolVersionMajor type="Integer" value="1"/>
0174	<ProtocolVersionMinor type="Integer" value="2"/>
0175	</ProtocolVersion>

0176	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0177	<BatchCount type="Integer" value="1"/>
0178	</ResponseHeader>
0179	<BatchItem>
0180	<Operation type="Enumeration" value="Activate"/>
0181	<ResultStatus type="Enumeration" value="Success"/>
0182	<ResponsePayload>
0183	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0184	</ResponsePayload>
0185	</BatchItem>
0186	</ResponseMessage>
	# TIME 3
0187	<RequestMessage>
0188	<RequestHeader>
0189	<ProtocolVersion>
0190	<ProtocolVersionMajor type="Integer" value="1"/>
0191	<ProtocolVersionMinor type="Integer" value="2"/>
0192	</ProtocolVersion>
0193	<BatchCount type="Integer" value="1"/>
0194	</RequestHeader>
0195	<BatchItem>
0196	<Operation type="Enumeration" value="GetAttributes"/>
0197	<RequestPayload>
0198	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0199	<AttributeName type="TextString" value="State"/>
0200	<AttributeName type="TextString" value="Activation Date"/>
0201	<AttributeName type="TextString" value="Deactivation Date"/>
0202	</RequestPayload>
0203	</BatchItem>
0204	</RequestMessage>
0205	<ResponseMessage>
0206	<ResponseHeader>
0207	<ProtocolVersion>
0208	<ProtocolVersionMajor type="Integer" value="1"/>
0209	<ProtocolVersionMinor type="Integer" value="2"/>
0210	</ProtocolVersion>
0211	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0212	<BatchCount type="Integer" value="1"/>
0213	</ResponseHeader>
0214	<BatchItem>
0215	<Operation type="Enumeration" value="GetAttributes"/>
0216	<ResultStatus type="Enumeration" value="Success"/>
0217	<ResponsePayload>
0218	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0219	<Attribute>
0220	<AttributeName type="TextString" value="State"/>
0221	<AttributeValue type="Enumeration" value="Active"/>
0222	</Attribute>
0223	<Attribute>
0224	<AttributeName type="TextString" value="Activation Date"/>
0225	<AttributeValue type="DateTime" value="2013-01-
	10T23:36:01+00:00"/>
0226	</Attribute>
0227	</ResponsePayload>
0228	</BatchItem>



0229	</ResponseMessage>
	# TIME 4
0230	<RequestMessage>
0231	<RequestHeader>
0232	<ProtocolVersion>
0233	<ProtocolVersionMajor type="Integer" value="1"/>
0234	<ProtocolVersionMinor type="Integer" value="2"/>
0235	</ProtocolVersion>
0236	<BatchCount type="Integer" value="1"/>
0237	</RequestHeader>
0238	<BatchItem>
0239	<Operation type="Enumeration" value="GetAttributes"/>
0240	<RequestPayload>
0241	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0242	<AttributeName type="TextString" value="State"/>
0243	<AttributeName type="TextString" value="Activation Date"/>
0244	<AttributeName type="TextString" value="Deactivation Date"/>
0245	</RequestPayload>
0246	</BatchItem>
0247	</RequestMessage>
0248	<ResponseMessage>
0249	<ResponseHeader>
0250	<ProtocolVersion>
0251	<ProtocolVersionMajor type="Integer" value="1"/>
0252	<ProtocolVersionMinor type="Integer" value="2"/>
0253	</ProtocolVersion>
0254	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0255	<BatchCount type="Integer" value="1"/>
0256	</ResponseHeader>
0257	<BatchItem>
0258	<Operation type="Enumeration" value="GetAttributes"/>
0259	<ResultStatus type="Enumeration" value="Success"/>
0260	<ResponsePayload>
0261	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0262	<Attribute>
0263	<AttributeName type="TextString" value="State"/>
0264	<AttributeValue type="Enumeration" value="PreActive"/>
0265	</Attribute>
0266	</ResponsePayload>
0267	</BatchItem>
0268	</ResponseMessage>
	# TIME 5
0269	<RequestMessage>
0270	<RequestHeader>
0271	<ProtocolVersion>
0272	<ProtocolVersionMajor type="Integer" value="1"/>
0273	<ProtocolVersionMinor type="Integer" value="2"/>
0274	</ProtocolVersion>
0275	<BatchCount type="Integer" value="1"/>
0276	</RequestHeader>
0277	<BatchItem>
0278	<Operation type="Enumeration" value="Destroy"/>
0279	<RequestPayload>
0280	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0281	</RequestPayload>

0282	</BatchItem>
0283	</RequestMessage>
0284	<ResponseMessage>
0285	<ResponseHeader>
0286	<ProtocolVersion>
0287	<ProtocolVersionMajor type="Integer" value="1"/>
0288	<ProtocolVersionMinor type="Integer" value="2"/>
0289	</ProtocolVersion>
0290	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0291	<BatchCount type="Integer" value="1"/>
0292	</ResponseHeader>
0293	<BatchItem>
0294	<Operation type="Enumeration" value="Destroy"/>
0295	<ResultStatus type="Enumeration" value="OperationFailed"/>
0296	<ResultReason type="Enumeration" value="PermissionDenied"/>
0297	<ResultMessage type="TextString" value="DENIED"/>
0298	</BatchItem>
0299	</ResponseMessage>
	# TIME 6
0300	<RequestMessage>
0301	<RequestHeader>
0302	<ProtocolVersion>
0303	<ProtocolVersionMajor type="Integer" value="1"/>
0304	<ProtocolVersionMinor type="Integer" value="2"/>
0305	</ProtocolVersion>
0306	<BatchCount type="Integer" value="1"/>
0307	</RequestHeader>
0308	<BatchItem>
0309	<Operation type="Enumeration" value="Destroy"/>
0310	<RequestPayload>
0311	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0312	</RequestPayload>
0313	</BatchItem>
0314	</RequestMessage>
0315	<ResponseMessage>
0316	<ResponseHeader>
0317	<ProtocolVersion>
0318	<ProtocolVersionMajor type="Integer" value="1"/>
0319	<ProtocolVersionMinor type="Integer" value="2"/>
0320	</ProtocolVersion>
0321	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0322	<BatchCount type="Integer" value="1"/>
0323	</ResponseHeader>
0324	<BatchItem>
0325	<Operation type="Enumeration" value="Destroy"/>
0326	<ResultStatus type="Enumeration" value="Success"/>
0327	<ResponsePayload>
0328	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0329	</ResponsePayload>
0330	</BatchItem>
0331	</ResponseMessage>
	# TIME 7
0332	<RequestMessage>
0333	<RequestHeader>
0334	<ProtocolVersion>
0335	<ProtocolVersionMajor type="Integer" value="1"/>

0336	<ProtocolVersionMinor type="Integer" value="2"/>
0337	</ProtocolVersion>
0338	<BatchCount type="Integer" value="1"/>
0339	</RequestHeader>
0340	<BatchItem>
0341	<Operation type="Enumeration" value="Revoke"/>
0342	<RequestPayload>
0343	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0344	<RevocationReason>
0345	<RevocationReasonCode type="Enumeration"
	value="KeyCompromise"/>
0346	</RevocationReason>
0347	<CompromiseOccurrenceDate type="DateTime" value="1970-01-
	01T00:00:06+00:00"/>
0348	</RequestPayload>
0349	</BatchItem>
0350	</RequestMessage>
0351	<ResponseMessage>
0352	<ResponseHeader>
0353	<ProtocolVersion>
0354	<ProtocolVersionMajor type="Integer" value="1"/>
0355	<ProtocolVersionMinor type="Integer" value="2"/>
0356	</ProtocolVersion>
0357	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0358	<BatchCount type="Integer" value="1"/>
0359	</ResponseHeader>
0360	<BatchItem>
0361	<Operation type="Enumeration" value="Revoke"/>
0362	<ResultStatus type="Enumeration" value="Success"/>
0363	<ResponsePayload>
0364	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0365	</ResponsePayload>
0366	</BatchItem>
0367	</ResponseMessage>
	<i># TIME 8</i>
0368	<RequestMessage>
0369	<RequestHeader>
0370	<ProtocolVersion>
0371	<ProtocolVersionMajor type="Integer" value="1"/>
0372	<ProtocolVersionMinor type="Integer" value="2"/>
0373	</ProtocolVersion>
0374	<BatchCount type="Integer" value="1"/>
0375	</RequestHeader>
0376	<BatchItem>
0377	<Operation type="Enumeration" value="GetAttributes"/>
0378	<RequestPayload>
0379	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0380	<AttributeName type="TextString" value="State"/>
0381	</RequestPayload>
0382	</BatchItem>
0383	</RequestMessage>
0384	<ResponseMessage>
0385	<ResponseHeader>
0386	<ProtocolVersion>
0387	<ProtocolVersionMajor type="Integer" value="1"/>

0388	<ProtocolVersionMinor type="Integer" value="2"/>
0389	</ProtocolVersion>
0390	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0391	<BatchCount type="Integer" value="1"/>
0392	</ResponseHeader>
0393	<BatchItem>
0394	<Operation type="Enumeration" value="GetAttributes"/>
0395	<ResultStatus type="Enumeration" value="Success"/>
0396	<ResponsePayload>
0397	<UniqueIdentifier type="TextString"
0398	value="\$UNIQUE_IDENTIFIER_0"/>
0399	<Attribute>
0400	<AttributeName type="TextString" value="State"/>
0401	<AttributeValue type="Enumeration" value="Compromised"/>
0402	</Attribute>
0403	</ResponsePayload>
0404	</BatchItem>
0405	</ResponseMessage>
0405	# TIME 9
0406	<RequestMessage>
0407	<RequestHeader>
0408	<ProtocolVersion>
0409	<ProtocolVersionMajor type="Integer" value="1"/>
0410	<ProtocolVersionMinor type="Integer" value="2"/>
0411	</ProtocolVersion>
0412	<BatchCount type="Integer" value="1"/>
0413	</RequestHeader>
0414	<BatchItem>
0415	<Operation type="Enumeration" value="Destroy"/>
0416	<RequestPayload>
0417	<UniqueIdentifier type="TextString"
0418	value="\$UNIQUE_IDENTIFIER_0"/>
0419	</RequestPayload>
0420	</BatchItem>
0421	</RequestMessage>
0422	<ResponseMessage>
0423	<ResponseHeader>
0424	<ProtocolVersion>
0425	<ProtocolVersionMajor type="Integer" value="1"/>
0426	<ProtocolVersionMinor type="Integer" value="2"/>
0427	</ProtocolVersion>
0428	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0429	<BatchCount type="Integer" value="1"/>
0430	</ResponseHeader>
0431	<BatchItem>
0432	<Operation type="Enumeration" value="Destroy"/>
0433	<ResultStatus type="Enumeration" value="Success"/>
0434	<ResponsePayload>
0435	<UniqueIdentifier type="TextString"
0436	value="\$UNIQUE_IDENTIFIER_0"/>

128 **3.3.3 AKLC-M-3-12**

129 CreateKeyPair, 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="CreateKeyPair"/>
0011     <RequestPayload>
0012       <CommonTemplateAttribute>
0013         <Attribute>
0014           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0015           <AttributeValue type="Enumeration" value="RSA"/>
0016         </Attribute>
0017         <Attribute>
0018           <AttributeName type="TextString" value="Cryptographic
Length"/>
0019           <AttributeValue type="Integer" value="2048"/>
0020         </Attribute>
0021       </CommonTemplateAttribute>
0022       <PrivateKeyTemplateAttribute>
0023         <Attribute>
0024           <AttributeName type="TextString" value="Name"/>
0025           <AttributeValue>
0026             <NameValuePair type="TextString" value="AKLC-M-3-12-
private"/>
0027             <NameType type="Enumeration"
value="UninterpretedTextString"/>
0028           </AttributeValue>
0029         </Attribute>
0030         <Attribute>
0031           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0032           <AttributeValue type="Integer" value="Sign"/>
0033         </Attribute>
0034       </PrivateKeyTemplateAttribute>
0035       <PublicKeyTemplateAttribute>
0036         <Attribute>
0037           <AttributeName type="TextString" value="Name"/>
0038           <AttributeValue>
0039             <NameValuePair type="TextString" value="AKLC-M-3-12-
public"/>
0040             <NameType type="Enumeration"
value="UninterpretedTextString"/>
0041           </AttributeValue>
0042         </Attribute>
0043         <Attribute>
0044           <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0045           <AttributeValue type="Integer" value="Verify"/>
0046         </Attribute>

```

0047	</PublicKeyTemplateAttribute>
0048	</RequestPayload>
0049	</BatchItem>
0050	</RequestMessage>
0051	<ResponseMessage>
0052	<ResponseHeader>
0053	<ProtocolVersion>
0054	<ProtocolVersionMajor type="Integer" value="1"/>
0055	<ProtocolVersionMinor type="Integer" value="2"/>
0056	</ProtocolVersion>
0057	<TimeStamp type="DateTime" value="2012-04-27T08:14:39+00:00"/>
0058	<BatchCount type="Integer" value="1"/>
0059	</ResponseHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="CreateKeyPair"/>
0062	<ResultStatus type="Enumeration" value="Success"/>
0063	<ResponsePayload>
0064	<PrivateKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0065	<PublicKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
0069	# TIME 1 <RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="2"/>
0074	</ProtocolVersion>
0075	<BatchCount type="Integer" value="1"/>
0076	</RequestHeader>
0077	<BatchItem>
0078	<Operation type="Enumeration" value="GetAttributes"/>
0079	<RequestPayload>
0080	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0081	<AttributeName type="TextString" value="State"/>
0082	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0083	<AttributeName type="TextString" value="Unique Identifier"/>
0084	<AttributeName type="TextString" value="Object Type"/>
0085	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0086	<AttributeName type="TextString" value="Cryptographic Length"/>
0087	<AttributeName type="TextString" value="Digest"/>
0088	<AttributeName type="TextString" value="Initial Date"/>
0089	<AttributeName type="TextString" value="Last Change Date"/>
0090	<AttributeName type="TextString" value="Original Creation Date"/>
0091	</RequestPayload>
0092	</BatchItem>
0093	</RequestMessage>
0094	<ResponseMessage>
0095	<ResponseHeader>
0096	<ProtocolVersion>

```

0097     <ProtocolVersionMajor type="Integer" value="1"/>
0098     <ProtocolVersionMinor type="Integer" value="2"/>
0099     </ProtocolVersion>
0100     <TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0101     <BatchCount type="Integer" value="1"/>
0102     </ResponseHeader>
0103     <BatchItem>
0104         <Operation type="Enumeration" value="GetAttributes"/>
0105         <ResultStatus type="Enumeration" value="Success"/>
0106         <ResponsePayload>
0107             <UniqueIdentifier type="TextString"
0108 value="$UNIQUE_IDENTIFIER_0"/>
0109             <Attribute>
0110                 <AttributeName type="TextString" value="State"/>
0111                 <AttributeValue type="Enumeration" value="PreActive"/>
0112             </Attribute>
0113             <Attribute>
0114                 <AttributeName type="TextString" value="Cryptographic Usage
0115 Mask"/>
0116                 <AttributeValue type="Integer" value="Sign"/>
0117             </Attribute>
0118             <Attribute>
0119                 <AttributeName type="TextString" value="Unique Identifier"/>
0120                 <AttributeValue type="TextString"
0121 value="$UNIQUE_IDENTIFIER_0"/>
0122             </Attribute>
0123             <Attribute>
0124                 <AttributeName type="TextString" value="Object Type"/>
0125                 <AttributeValue type="Enumeration" value="PrivateKey"/>
0126             </Attribute>
0127             <Attribute>
0128                 <AttributeName type="TextString" value="Cryptographic
0129 Algorithm"/>
0130                 <AttributeValue type="Enumeration" value="RSA"/>
0131             </Attribute>
0132             <Attribute>
0133                 <AttributeName type="TextString" value="Cryptographic
0134 Length"/>
0135                 <AttributeValue type="Integer" value="2048"/>
0136             </Attribute>
0137             <Attribute>
0138                 <AttributeName type="TextString" value="Digest"/>
0139                 <AttributeValue>
0140                     <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0141                     <DigestValue type="ByteString"
0142 value="8eb422ae2b006a05d3c8a542a28536735241b6dc1c37926bc8007bd6220d9
0143 230"/>
0144                 </AttributeValue>
0145             </Attribute>
0146             <Attribute>
0147                 <AttributeName type="TextString" value="Initial Date"/>
0148                 <AttributeValue type="DateTime" value="2013-01-
0149 11T08:18:21+00:00"/>
0150             </Attribute>
0151             <Attribute>
0152                 <AttributeName type="TextString" value="Last Change Date"/>
0153                 <AttributeValue type="DateTime" value="2013-01-

```

0147	11T08:18:21+00:00"/>
0148	</Attribute>
0149	<Attribute type="TextString" value="Original Creation Date"/>
0150	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0151	</Attribute>
0152	</ResponsePayload>
0153	</BatchItem>
0154	</ResponseMessage>
0155	# TIME 2 <RequestMessage>
0156	<RequestHeader>
0157	<ProtocolVersion>
0158	<ProtocolVersionMajor type="Integer" value="1"/>
0159	<ProtocolVersionMinor type="Integer" value="2"/>
0160	</ProtocolVersion>
0161	<BatchCount type="Integer" value="1"/>
0162	</RequestHeader>
0163	<BatchItem>
0164	<Operation type="Enumeration" value="Activate"/>
0165	<RequestPayload>
0166	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0167	</RequestPayload>
0168	</BatchItem>
0169	</RequestMessage>
0170	<ResponseMessage>
0171	<ResponseHeader>
0172	<ProtocolVersion>
0173	<ProtocolVersionMajor type="Integer" value="1"/>
0174	<ProtocolVersionMinor type="Integer" value="2"/>
0175	</ProtocolVersion>
0176	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0177	<BatchCount type="Integer" value="1"/>
0178	</ResponseHeader>
0179	<BatchItem>
0180	<Operation type="Enumeration" value="Activate"/>
0181	<ResultStatus type="Enumeration" value="Success"/>
0182	<ResponsePayload>
0183	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0184	</ResponsePayload>
0185	</BatchItem>
0186	</ResponseMessage>
0187	# TIME 3 <RequestMessage>
0188	<RequestHeader>
0189	<ProtocolVersion>
0190	<ProtocolVersionMajor type="Integer" value="1"/>
0191	<ProtocolVersionMinor type="Integer" value="2"/>
0192	</ProtocolVersion>
0193	<BatchCount type="Integer" value="1"/>
0194	</RequestHeader>
0195	<BatchItem>
0196	<Operation type="Enumeration" value="GetAttributes"/>
0197	<RequestPayload>



0198	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0199	<AttributeName type="TextString" value="State"/>
0200	<AttributeName type="TextString" value="Activation Date"/>
0201	<AttributeName type="TextString" value="Deactivation Date"/>
0202	</RequestPayload>
0203	</BatchItem>
0204	</RequestMessage>
0205	<ResponseMessage>
0206	<ResponseHeader>
0207	<ProtocolVersion>
0208	<ProtocolVersionMajor type="Integer" value="1"/>
0209	<ProtocolVersionMinor type="Integer" value="2"/>
0210	</ProtocolVersion>
0211	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0212	<BatchCount type="Integer" value="1"/>
0213	</ResponseHeader>
0214	<BatchItem>
0215	<Operation type="Enumeration" value="GetAttributes"/>
0216	<ResultStatus type="Enumeration" value="Success"/>
0217	<ResponsePayload>
0218	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0219	<Attribute>
0220	<AttributeName type="TextString" value="State"/>
0221	<AttributeValue type="Enumeration" value="Active"/>
0222	</Attribute>
0223	<Attribute>
0224	<AttributeName type="TextString" value="Activation Date"/>
0225	<AttributeValue type="DateTime" value="2013-01- 10T23:36:01+00:00"/>
0226	</Attribute>
0227	</ResponsePayload>
0228	</BatchItem>
0229	</ResponseMessage>
0230	# TIME 4 <RequestMessage>
0231	<RequestHeader>
0232	<ProtocolVersion>
0233	<ProtocolVersionMajor type="Integer" value="1"/>
0234	<ProtocolVersionMinor type="Integer" value="2"/>
0235	</ProtocolVersion>
0236	<BatchCount type="Integer" value="1"/>
0237	</RequestHeader>
0238	<BatchItem>
0239	<Operation type="Enumeration" value="ModifyAttribute"/>
0240	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0241	<RequestPayload>
0242	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0243	<Attribute>
0244	<AttributeName type="TextString" value="Activation Date"/>
0245	<AttributeValue type="DateTime" value="\$NOW"/>
0246	</Attribute>
0247	</RequestPayload>
0248	</BatchItem>
0249	</RequestMessage>
0250	<ResponseMessage>

0251	<ResponseHeader>
0252	<ProtocolVersion>
0253	<ProtocolVersionMajor type="Integer" value="1"/>
0254	<ProtocolVersionMinor type="Integer" value="2"/>
0255	</ProtocolVersion>
0256	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0257	<BatchCount type="Integer" value="1"/>
0258	</ResponseHeader>
0259	<BatchItem>
0260	<Operation type="Enumeration" value="ModifyAttribute"/>
0261	<UniqueBatchItemID type="ByteString" value="0752c951bb9926cc"/>
0262	<ResultStatus type="Enumeration" value="OperationFailed"/>
0263	<ResultReason type="Enumeration" value="PermissionDenied"/>
0264	<ResultMessage type="TextString" value="DENIED"/>
0265	</BatchItem>
0266	</ResponseMessage>
	# TIME 5
0267	<RequestMessage>
0268	<RequestHeader>
0269	<ProtocolVersion>
0270	<ProtocolVersionMajor type="Integer" value="1"/>
0271	<ProtocolVersionMinor type="Integer" value="2"/>
0272	</ProtocolVersion>
0273	<BatchCount type="Integer" value="1"/>
0274	</RequestHeader>
0275	<BatchItem>
0276	<Operation type="Enumeration" value="Revoke"/>
0277	<RequestPayload>
0278	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0279	<RevocationReason>
0280	<RevocationReasonCode type="Enumeration"
	value="KeyCompromise"/>
0281	</RevocationReason>
0282	<CompromiseOccurrenceDate type="DateTime" value="1970-01-
	01T00:00:06+00:00"/>
0283	</RequestPayload>
0284	</BatchItem>
0285	</RequestMessage>
0286	<ResponseMessage>
0287	<ResponseHeader>
0288	<ProtocolVersion>
0289	<ProtocolVersionMajor type="Integer" value="1"/>
0290	<ProtocolVersionMinor type="Integer" value="2"/>
0291	</ProtocolVersion>
0292	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0293	<BatchCount type="Integer" value="1"/>
0294	</ResponseHeader>
0295	<BatchItem>
0296	<Operation type="Enumeration" value="Revoke"/>
0297	<ResultStatus type="Enumeration" value="Success"/>
0298	<ResponsePayload>
0299	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0300	</ResponsePayload>
0301	</BatchItem>
0302	</ResponseMessage>
	# TIME 6

0303	<RequestMessage>
0304	<RequestHeader>
0305	<ProtocolVersion>
0306	<ProtocolVersionMajor type="Integer" value="1"/>
0307	<ProtocolVersionMinor type="Integer" value="2"/>
0308	</ProtocolVersion>
0309	<BatchCount type="Integer" value="1"/>
0310	</RequestHeader>
0311	<BatchItem>
0312	<Operation type="Enumeration" value="GetAttributes"/>
0313	<RequestPayload>
0314	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0315	<AttributeName type="TextString" value="State"/>
0316	</RequestPayload>
0317	</BatchItem>
0318	</RequestMessage>
0319	<ResponseMessage>
0320	<ResponseHeader>
0321	<ProtocolVersion>
0322	<ProtocolVersionMajor type="Integer" value="1"/>
0323	<ProtocolVersionMinor type="Integer" value="2"/>
0324	</ProtocolVersion>
0325	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0326	<BatchCount type="Integer" value="1"/>
0327	</ResponseHeader>
0328	<BatchItem>
0329	<Operation type="Enumeration" value="GetAttributes"/>
0330	<ResultStatus type="Enumeration" value="Success"/>
0331	<ResponsePayload>
0332	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0333	<Attribute>
0334	<AttributeName type="TextString" value="State"/>
0335	<AttributeValue type="Enumeration" value="Compromised"/>
0336	</Attribute>
0337	</ResponsePayload>
0338	</BatchItem>
0339	</ResponseMessage>
	# TIME 7
0340	<RequestMessage>
0341	<RequestHeader>
0342	<ProtocolVersion>
0343	<ProtocolVersionMajor type="Integer" value="1"/>
0344	<ProtocolVersionMinor type="Integer" value="2"/>
0345	</ProtocolVersion>
0346	<BatchCount type="Integer" value="1"/>
0347	</RequestHeader>
0348	<BatchItem>
0349	<Operation type="Enumeration" value="GetAttributes"/>
0350	<RequestPayload>
0351	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0352	<AttributeName type="TextString" value="State"/>
0353	</RequestPayload>
0354	</BatchItem>
0355	</RequestMessage>
0356	<ResponseMessage>

0357	<ResponseHeader>
0358	<ProtocolVersion>
0359	<ProtocolVersionMajor type="Integer" value="1"/>
0360	<ProtocolVersionMinor type="Integer" value="2"/>
0361	</ProtocolVersion>
0362	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0363	<BatchCount type="Integer" value="1"/>
0364	</ResponseHeader>
0365	<BatchItem>
0366	<Operation type="Enumeration" value="GetAttributes"/>
0367	<ResultStatus type="Enumeration" value="Success"/>
0368	<ResponsePayload>
0369	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0370	<Attribute>
0371	<AttributeName type="TextString" value="State"/>
0372	<AttributeValue type="Enumeration" value="PreActive"/>
0373	</Attribute>
0374	</ResponsePayload>
0375	</BatchItem>
0376	</ResponseMessage>
	# TIME 8
0377	<RequestMessage>
0378	<RequestHeader>
0379	<ProtocolVersion>
0380	<ProtocolVersionMajor type="Integer" value="1"/>
0381	<ProtocolVersionMinor type="Integer" value="2"/>
0382	</ProtocolVersion>
0383	<BatchCount type="Integer" value="1"/>
0384	</RequestHeader>
0385	<BatchItem>
0386	<Operation type="Enumeration" value="Destroy"/>
0387	<RequestPayload>
0388	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0389	</RequestPayload>
0390	</BatchItem>
0391	</RequestMessage>
0392	<ResponseMessage>
0393	<ResponseHeader>
0394	<ProtocolVersion>
0395	<ProtocolVersionMajor type="Integer" value="1"/>
0396	<ProtocolVersionMinor type="Integer" value="2"/>
0397	</ProtocolVersion>
0398	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0399	<BatchCount type="Integer" value="1"/>
0400	</ResponseHeader>
0401	<BatchItem>
0402	<Operation type="Enumeration" value="Destroy"/>
0403	<ResultStatus type="Enumeration" value="Success"/>
0404	<ResponsePayload>
0405	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0406	</ResponsePayload>
0407	</BatchItem>
0408	</ResponseMessage>
	# TIME 9
0409	<RequestMessage>

0410	<RequestHeader>
0411	<ProtocolVersion>
0412	<ProtocolVersionMajor type="Integer" value="1"/>
0413	<ProtocolVersionMinor type="Integer" value="2"/>
0414	</ProtocolVersion>
0415	<BatchCount type="Integer" value="1"/>
0416	</RequestHeader>
0417	<BatchItem>
0418	<Operation type="Enumeration" value="Destroy"/>
0419	<RequestPayload>
0420	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0421	</RequestPayload>
0422	</BatchItem>
0423	</RequestMessage>
0424	<ResponseMessage>
0425	<ResponseHeader>
0426	<ProtocolVersion>
0427	<ProtocolVersionMajor type="Integer" value="1"/>
0428	<ProtocolVersionMinor type="Integer" value="2"/>
0429	</ProtocolVersion>
0430	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0431	<BatchCount type="Integer" value="1"/>
0432	</ResponseHeader>
0433	<BatchItem>
0434	<Operation type="Enumeration" value="Destroy"/>
0435	<ResultStatus type="Enumeration" value="Success"/>
0436	<ResponsePayload>
0437	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0438	</ResponsePayload>
0439	</BatchItem>
0440	</ResponseMessage>

130

## 131 3.4 Optional Test Cases KMIP v1.0

### 132 3.4.1 AKLC-O-1-10

133 CreateKeyPair, 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="CreateKeyPair"/>
0011	<RequestPayload>
0012	<CommonTemplateAttribute>
0013	<Attribute>
0014	<AttributeName type="TextString" value="Cryptographic"
	Algorithm"/>
0015	<AttributeValue type="Enumeration" value="RSA"/>

```

0016         </Attribute>
0017         <Attribute>
0018             <AttributeName type="TextString" value="Cryptographic
Length"/>
0019             <AttributeValue type="Integer" value="2048"/>
0020         </Attribute>
0021     </CommonTemplateAttribute>
0022     <PrivateKeyTemplateAttribute>
0023         <Attribute>
0024             <AttributeName type="TextString" value="Name"/>
0025             <AttributeValue>
0026                 <NameValue type="TextString" value="AKLC-O-1-10-
private"/>
0027                 <NameType type="Enumeration"
value="UninterpretedTextString"/>
0028             </AttributeValue>
0029         </Attribute>
0030         <Attribute>
0031             <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0032             <AttributeValue type="Integer" value="Sign"/>
0033         </Attribute>
0034     </PrivateKeyTemplateAttribute>
0035     <PublicKeyTemplateAttribute>
0036         <Attribute>
0037             <AttributeName type="TextString" value="Name"/>
0038             <AttributeValue>
0039                 <NameValue type="TextString" value="AKLC-O-1-10-
public"/>
0040                 <NameType type="Enumeration"
value="UninterpretedTextString"/>
0041             </AttributeValue>
0042         </Attribute>
0043         <Attribute>
0044             <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0045             <AttributeValue type="Integer" value="Verify"/>
0046         </Attribute>
0047     </PublicKeyTemplateAttribute>
0048 </RequestPayload>
0049 </BatchItem>
0050 </RequestMessage>
0051 <ResponseMessage>
0052     <ResponseHeader>
0053         <ProtocolVersion>
0054             <ProtocolVersionMajor type="Integer" value="1"/>
0055             <ProtocolVersionMinor type="Integer" value="0"/>
0056         </ProtocolVersion>
0057         <TimeStamp type="DateTime" value="2013-01-11T08:32:04+00:00"/>
0058         <BatchCount type="Integer" value="1"/>
0059     </ResponseHeader>
0060     <BatchItem>
0061         <Operation type="Enumeration" value="CreateKeyPair"/>
0062         <ResultStatus type="Enumeration" value="Success"/>
0063     <ResponsePayload>
0064         <PrivateKeyUniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0065         <PublicKeyUniqueIdentifier type="TextString"

```

0066	value="\$UNIQUE_IDENTIFIER_1"/>
0067	</ResponsePayload>
0068	</BatchItem>
	</ResponseMessage>
	# TIME 1
0069	<RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>
0072	<ProtocolVersionMajor type="Integer" value="1"/>
0073	<ProtocolVersionMinor type="Integer" value="0"/>
0074	</ProtocolVersion>
0075	<BatchCount type="Integer" value="1"/>
0076	</RequestHeader>
0077	<BatchItem>
0078	<Operation type="Enumeration" value="GetAttributes"/>
0079	<RequestPayload>
0080	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0081	<AttributeName type="TextString" value="State"/>
0082	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0083	<AttributeName type="TextString" value="Unique Identifier"/>
0084	<AttributeName type="TextString" value="Object Type"/>
0085	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0086	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0087	<AttributeName type="TextString" value="Digest"/>
0088	<AttributeName type="TextString" value="Initial Date"/>
0089	<AttributeName type="TextString" value="Last Change Date"/>
0090	<AttributeName type="TextString" value="Activation Date"/>
0091	</RequestPayload>
0092	</BatchItem>
0093	</RequestMessage>
0094	<ResponseMessage>
0095	<ResponseHeader>
0096	<ProtocolVersion>
0097	<ProtocolVersionMajor type="Integer" value="1"/>
0098	<ProtocolVersionMinor type="Integer" value="0"/>
0099	</ProtocolVersion>
0100	<TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0101	<BatchCount type="Integer" value="1"/>
0102	</ResponseHeader>
0103	<BatchItem>
0104	<Operation type="Enumeration" value="GetAttributes"/>
0105	<ResultStatus type="Enumeration" value="Success"/>
0106	<ResponsePayload>
0107	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0108	<Attribute>
0109	<AttributeName type="TextString" value="State"/>
0110	<AttributeValue type="Enumeration" value="PreActive"/>
0111	</Attribute>
0112	<Attribute>
0113	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0114	<AttributeValue type="Integer" value="Sign"/>
0115	</Attribute>

```

0116     <Attribute>
0117         <AttributeName type="TextString" value="Unique Identifier"/>
0118         <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0119     </Attribute>
0120     <Attribute>
0121         <AttributeName type="TextString" value="Object Type"/>
0122         <AttributeValue type="Enumeration" value="PrivateKey"/>
0123     </Attribute>
0124     <Attribute>
0125         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0126         <AttributeValue type="Enumeration" value="RSA"/>
0127     </Attribute>
0128     <Attribute>
0129         <AttributeName type="TextString" value="Cryptographic
Length"/>
0130         <AttributeValue type="Integer" value="2048"/>
0131     </Attribute>
0132     <Attribute>
0133         <AttributeName type="TextString" value="Digest"/>
0134         <AttributeValue>
0135             <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0136             <DigestValue type="ByteString"
value="8eb422ae2b006a05d3c8a542a28536735241b6dc1c37926bc8007bd6220d9
230"/>
0137         </AttributeValue>
0138     </Attribute>
0139     <Attribute>
0140         <AttributeName type="TextString" value="Initial Date"/>
0141         <AttributeValue type="DateTime" value="2013-01-
11T08:18:21+00:00"/>
0142     </Attribute>
0143     <Attribute>
0144         <AttributeName type="TextString" value="Last Change Date"/>
0145         <AttributeValue type="DateTime" value="2013-01-
11T08:18:21+00:00"/>
0146     </Attribute>
0147 </ResponsePayload>
0148 </BatchItem>
0149 </ResponseMessage>
# TIME 2
0150 <RequestMessage>
0151     <RequestHeader>
0152         <ProtocolVersion>
0153             <ProtocolVersionMajor type="Integer" value="1"/>
0154             <ProtocolVersionMinor type="Integer" value="0"/>
0155         </ProtocolVersion>
0156         <BatchCount type="Integer" value="1"/>
0157     </RequestHeader>
0158     <BatchItem>
0159         <Operation type="Enumeration" value="Destroy"/>
0160         <RequestPayload>
0161             <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0162         </RequestPayload>
0163     </BatchItem>
0164 </RequestMessage>

```



0165	<ResponseMessage>
0166	<ResponseHeader>
0167	<ProtocolVersion>
0168	<ProtocolVersionMajor type="Integer" value="1"/>
0169	<ProtocolVersionMinor type="Integer" value="0"/>
0170	</ProtocolVersion>
0171	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0172	<BatchCount type="Integer" value="1"/>
0173	</ResponseHeader>
0174	<BatchItem>
0175	<Operation type="Enumeration" value="Destroy"/>
0176	<ResultStatus type="Enumeration" value="Success"/>
0177	<ResponsePayload>
0178	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0179	</ResponsePayload>
0180	</BatchItem>
0181	</ResponseMessage>
	# TIME 3
0182	<RequestMessage>
0183	<RequestHeader>
0184	<ProtocolVersion>
0185	<ProtocolVersionMajor type="Integer" value="1"/>
0186	<ProtocolVersionMinor type="Integer" value="0"/>
0187	</ProtocolVersion>
0188	<BatchCount type="Integer" value="1"/>
0189	</RequestHeader>
0190	<BatchItem>
0191	<Operation type="Enumeration" value="GetAttributes"/>
0192	<RequestPayload>
0193	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0194	</RequestPayload>
0195	</BatchItem>
0196	</RequestMessage>
0197	<ResponseMessage>
0198	<ResponseHeader>
0199	<ProtocolVersion>
0200	<ProtocolVersionMajor type="Integer" value="1"/>
0201	<ProtocolVersionMinor type="Integer" value="0"/>
0202	</ProtocolVersion>
0203	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0204	<BatchCount type="Integer" value="1"/>
0205	</ResponseHeader>
0206	<BatchItem>
0207	<Operation type="Enumeration" value="GetAttributes"/>
0208	<ResultStatus type="Enumeration" value="Success"/>
0209	<ResponsePayload>
0210	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0211	<Attribute>
0212	<AttributeName type="TextString" value="Unique Identifier"/>
0213	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0214	</Attribute>
0215	<Attribute>
0216	<AttributeName type="TextString" value="Object Type"/>
0217	<AttributeValue type="Enumeration" value="PrivateKey"/>

```

0218     </Attribute>
0219     <Attribute>
0220         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0221         <AttributeValue type="Enumeration" value="RSA"/>
0222     </Attribute>
0223     <Attribute>
0224         <AttributeName type="TextString" value="Cryptographic
Length"/>
0225         <AttributeValue type="Integer" value="2048"/>
0226     </Attribute>
0227     <Attribute>
0228         <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0229         <AttributeValue type="Integer" value="Sign"/>
0230     </Attribute>
0231     <Attribute>
0232         <AttributeName type="TextString" value="Destroy Date"/>
0233         <AttributeValue type="DateTime" value="2013-01-
11T08:40:05+00:00"/>
0234     </Attribute>
0235     <Attribute>
0236         <AttributeName type="TextString" value="Digest"/>
0237         <AttributeValue>
0238             <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0239             <DigestValue type="ByteString"
value="4abc48c2ba00a6bba22cb6fc2827b46107354968872b395edb31354e78878
be6"/>
0240         </AttributeValue>
0241     </Attribute>
0242     <Attribute>
0243         <AttributeName type="TextString" value="Initial Date"/>
0244         <AttributeValue type="DateTime" value="2013-01-
11T08:40:05+00:00"/>
0245     </Attribute>
0246     <Attribute>
0247         <AttributeName type="TextString" value="Last Change Date"/>
0248         <AttributeValue type="DateTime" value="2013-01-
11T08:40:05+00:00"/>
0249     </Attribute>
0250     <Attribute>
0251         <AttributeName type="TextString" value="Lease Time"/>
0252         <AttributeValue type="Interval" value="3600"/>
0253     </Attribute>
0254     <Attribute>
0255         <AttributeName type="TextString" value="Link"/>
0256         <AttributeValue>
0257             <LinkType type="Enumeration" value="PublicKeyLink"/>
0258             <LinkedObjectIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0259         </AttributeValue>
0260     </Attribute>
0261     <Attribute>
0262         <AttributeName type="TextString" value="Name"/>
0263         <AttributeValue>
0264             <NameValue type="TextString" value="AKLC-O-1-10-private"/>
0265             <NameType type="Enumeration"
value="UninterpretedTextString"/>

```

0266	</AttributeValue>
0267	</Attribute>
0268	<Attribute>
0269	<AttributeName type="TextString" value="State"/>
0270	<AttributeValue type="Enumeration" value="Destroyed"/>
0271	</Attribute>
0272	</ResponsePayload>
0273	</BatchItem>
0274	</ResponseMessage>
# TIME 4	
0275	<RequestMessage>
0276	<RequestHeader>
0277	<ProtocolVersion>
0278	<ProtocolVersionMajor type="Integer" value="1"/>
0279	<ProtocolVersionMinor type="Integer" value="0"/>
0280	</ProtocolVersion>
0281	<BatchCount type="Integer" value="1"/>
0282	</RequestHeader>
0283	<BatchItem>
0284	<Operation type="Enumeration" value="GetAttributes"/>
0285	<RequestPayload>
0286	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0287	</RequestPayload>
0288	</BatchItem>
0289	</RequestMessage>
0290	<ResponseMessage>
0291	<ResponseHeader>
0292	<ProtocolVersion>
0293	<ProtocolVersionMajor type="Integer" value="1"/>
0294	<ProtocolVersionMinor type="Integer" value="0"/>
0295	</ProtocolVersion>
0296	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0297	<BatchCount type="Integer" value="1"/>
0298	</ResponseHeader>
0299	<BatchItem>
0300	<Operation type="Enumeration" value="GetAttributes"/>
0301	<ResultStatus type="Enumeration" value="Success"/>
0302	<ResponsePayload>
0303	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0304	<Attribute>
0305	<AttributeName type="TextString" value="Unique Identifier"/>
0306	<AttributeValue type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0307	</Attribute>
0308	<Attribute>
0309	<AttributeName type="TextString" value="Object Type"/>
0310	<AttributeValue type="Enumeration" value="PublicKey"/>
0311	</Attribute>
0312	<Attribute>
0313	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0314	<AttributeValue type="Enumeration" value="RSA"/>
0315	</Attribute>
0316	<Attribute>
0317	<AttributeName type="TextString" value="Cryptographic Length"/>

0318	<AttributeValue type="Integer" value="2048"/>
0319	</Attribute>
0320	<Attribute>
0321	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0322	<AttributeValue type="Integer" value="Verify"/>
0323	</Attribute>
0324	<Attribute>
0325	<AttributeName type="TextString" value="Digest"/>
0326	<AttributeValue>
0327	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0328	<DigestValue type="ByteString" value="330306b0e337e32dd1b5acf92cb96fd39adb802f305e7406062248324816f445"/>
0329	</AttributeValue>
0330	</Attribute>
0331	<Attribute>
0332	<AttributeName type="TextString" value="Initial Date"/>
0333	<AttributeValue type="DateTime" value="2013-01-11T08:37:43+00:00"/>
0334	</Attribute>
0335	<Attribute>
0336	<AttributeName type="TextString" value="Last Change Date"/>
0337	<AttributeValue type="DateTime" value="2013-01-11T08:37:43+00:00"/>
0338	</Attribute>
0339	<Attribute>
0340	<AttributeName type="TextString" value="Lease Time"/>
0341	<AttributeValue type="Interval" value="3600"/>
0342	</Attribute>
0343	<Attribute>
0344	<AttributeName type="TextString" value="Link"/>
0345	<AttributeValue>
0346	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0347	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0348	</AttributeValue>
0349	</Attribute>
0350	<Attribute>
0351	<AttributeName type="TextString" value="Name"/>
0352	<AttributeValue>
0353	<NameValue type="TextString" value="AKLC-O-1-10-public"/>
0354	<NameType type="Enumeration" value="UninterpretedTextString"/>
0355	</AttributeValue>
0356	</Attribute>
0357	<Attribute>
0358	<AttributeName type="TextString" value="State"/>
0359	<AttributeValue type="Enumeration" value="PreActive"/>
0360	</Attribute>
0361	</ResponsePayload>
0362	</BatchItem>
0363	</ResponseMessage>
	# TIME 5
0364	<RequestMessage>
0365	<RequestHeader>
0366	<ProtocolVersion>
0367	<ProtocolVersionMajor type="Integer" value="1"/>

0368	<ProtocolVersionMinor type="Integer" value="0"/>
0369	</ProtocolVersion>
0370	<BatchCount type="Integer" value="1"/>
0371	</RequestHeader>
0372	<BatchItem>
0373	<Operation type="Enumeration" value="Destroy"/>
0374	<RequestPayload>
0375	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0376	</RequestPayload>
0377	</BatchItem>
0378	</RequestMessage>
0379	<ResponseMessage>
0380	<ResponseHeader>
0381	<ProtocolVersion>
0382	<ProtocolVersionMajor type="Integer" value="1"/>
0383	<ProtocolVersionMinor type="Integer" value="0"/>
0384	</ProtocolVersion>
0385	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0386	<BatchCount type="Integer" value="1"/>
0387	</ResponseHeader>
0388	<BatchItem>
0389	<Operation type="Enumeration" value="Destroy"/>
0390	<ResultStatus type="Enumeration" value="Success"/>
0391	<ResponsePayload>
0392	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0393	</ResponsePayload>
0394	</BatchItem>
0395	</ResponseMessage>
0396	<i># TIME 6</i> <RequestMessage>
0397	<RequestHeader>
0398	<ProtocolVersion>
0399	<ProtocolVersionMajor type="Integer" value="1"/>
0400	<ProtocolVersionMinor type="Integer" value="0"/>
0401	</ProtocolVersion>
0402	<BatchCount type="Integer" value="1"/>
0403	</RequestHeader>
0404	<BatchItem>
0405	<Operation type="Enumeration" value="GetAttributes"/>
0406	<RequestPayload>
0407	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0408	</RequestPayload>
0409	</BatchItem>
0410	</RequestMessage>
0411	<ResponseMessage>
0412	<ResponseHeader>
0413	<ProtocolVersion>
0414	<ProtocolVersionMajor type="Integer" value="1"/>
0415	<ProtocolVersionMinor type="Integer" value="0"/>
0416	</ProtocolVersion>
0417	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0418	<BatchCount type="Integer" value="1"/>
0419	</ResponseHeader>
0420	<BatchItem>
0421	<Operation type="Enumeration" value="GetAttributes"/>

```

0422     <ResultStatus type="Enumeration" value="Success"/>
0423     <ResponsePayload>
0424         <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0425         <Attribute>
0426             <AttributeName type="TextString" value="Unique Identifier"/>
0427             <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0428         </Attribute>
0429         <Attribute>
0430             <AttributeName type="TextString" value="Object Type"/>
0431             <AttributeValue type="Enumeration" value="PublicKey"/>
0432         </Attribute>
0433         <Attribute>
0434             <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0435             <AttributeValue type="Enumeration" value="RSA"/>
0436         </Attribute>
0437         <Attribute>
0438             <AttributeName type="TextString" value="Cryptographic
Length"/>
0439             <AttributeValue type="Integer" value="2048"/>
0440         </Attribute>
0441         <Attribute>
0442             <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0443             <AttributeValue type="Integer" value="Verify"/>
0444         </Attribute>
0445         <Attribute>
0446             <AttributeName type="TextString" value="Destroy Date"/>
0447             <AttributeValue type="DateTime" value="2013-01-
11T08:38:18+00:00"/>
0448         </Attribute>
0449         <Attribute>
0450             <AttributeName type="TextString" value="Digest"/>
0451             <AttributeValue>
0452                 <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0453                 <DigestValue type="ByteString"
value="b06f3e3d107a282adb5fe316356d13679d7cf7429d14a6f20665f45ba4d28
83c"/>
0454             </AttributeValue>
0455         </Attribute>
0456         <Attribute>
0457             <AttributeName type="TextString" value="Initial Date"/>
0458             <AttributeValue type="DateTime" value="2013-01-
11T08:38:18+00:00"/>
0459         </Attribute>
0460         <Attribute>
0461             <AttributeName type="TextString" value="Last Change Date"/>
0462             <AttributeValue type="DateTime" value="2013-01-
11T08:38:18+00:00"/>
0463         </Attribute>
0464         <Attribute>
0465             <AttributeName type="TextString" value="Lease Time"/>
0466             <AttributeValue type="Interval" value="3600"/>
0467         </Attribute>
0468         <Attribute>
0469             <AttributeName type="TextString" value="Link"/>

```

```

0470     <AttributeValue>
0471     <LinkType type="Enumeration" value="PrivateKeyLink"/>
0472     <LinkedObjectIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0473     </AttributeValue>
0474     </Attribute>
0475     <Attribute>
0476     <AttributeName type="TextString" value="Name"/>
0477     <AttributeValue>
0478     <NameValue type="TextString" value="AKLC-O-1-10-public"/>
0479     <NameType type="Enumeration"
value="UninterpretedTextString"/>
0480     </AttributeValue>
0481     </Attribute>
0482     <Attribute>
0483     <AttributeName type="TextString" value="State"/>
0484     <AttributeValue type="Enumeration" value="Destroyed"/>
0485     </Attribute>
0486     </ResponsePayload>
0487     </BatchItem>
0488     </ResponseMessage>

```

134

### 135 3.5 Optional Test Cases KMIP v1.1

#### 136 3.5.1 AKLC-O-1-11

137 CreateKeyPair, GetAttributes, Destroy, GetAttributes

```

# TIME 0
0001 <RequestMessage>
0002 <RequestHeader>
0003 <ProtocolVersion>
0004 <ProtocolVersionMajor type="Integer" value="1"/>
0005 <ProtocolVersionMinor type="Integer" value="1"/>
0006 </ProtocolVersion>
0007 <BatchCount type="Integer" value="1"/>
0008 </RequestHeader>
0009 <BatchItem>
0010 <Operation type="Enumeration" value="CreateKeyPair"/>
0011 <RequestPayload>
0012 <CommonTemplateAttribute>
0013 <Attribute>
0014 <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0015 <AttributeValue type="Enumeration" value="RSA"/>
0016 </Attribute>
0017 <Attribute>
0018 <AttributeName type="TextString" value="Cryptographic
Length"/>
0019 <AttributeValue type="Integer" value="2048"/>
0020 </Attribute>
0021 </CommonTemplateAttribute>
0022 <PrivateKeyTemplateAttribute>
0023 <Attribute>
0024 <AttributeName type="TextString" value="Name"/>
0025 <AttributeValue>
0026 <NameValue type="TextString" value="AKLC-O-1-11-

```

0027	private"/>
0028	<NameType type="Enumeration"
0029	value="UninterpretedTextString"/>
0030	</AttributeValue>
0031	</Attribute>
0032	<Attribute type="TextString" value="Cryptographic"
0033	Usage Mask"/>
0034	<AttributeValue type="Integer" value="Sign"/>
0035	</Attribute>
0036	</PrivateKeyTemplateAttribute>
0037	<PublicKeyTemplateAttribute>
0038	<Attribute>
0039	<AttributeName type="TextString" value="Name"/>
0040	<AttributeValue>
0041	<NameValue type="TextString" value="AKLC-O-1-11-
0042	public"/>
0043	<NameType type="Enumeration"
0044	value="UninterpretedTextString"/>
0045	</AttributeValue>
0046	</Attribute>
0047	<Attribute>
0048	<AttributeName type="TextString" value="Cryptographic"
0049	Usage Mask"/>
0050	<AttributeValue type="Integer" value="Verify"/>
0051	</Attribute>
0052	</PublicKeyTemplateAttribute>
0053	</RequestPayload>
0054	</BatchItem>
0055	</RequestMessage>
0056	</ResponseMessage>
0057	<ResponseHeader>
0058	<ProtocolVersion>
0059	<ProtocolVersionMajor type="Integer" value="1"/>
0060	<ProtocolVersionMinor type="Integer" value="1"/>
0061	</ProtocolVersion>
0062	<TimeStamp type="DateTime" value="2013-01-11T08:32:04+00:00"/>
0063	<BatchCount type="Integer" value="1"/>
0064	</ResponseHeader>
0065	<BatchItem>
0066	<Operation type="Enumeration" value="CreateKeyPair"/>
0067	<ResultStatus type="Enumeration" value="Success"/>
0068	<ResponsePayload>
0069	<PrivateKeyUniqueIdentifier type="TextString"
0070	value="\$UNIQUE_IDENTIFIER_0"/>
0071	<PublicKeyUniqueIdentifier type="TextString"
0072	value="\$UNIQUE_IDENTIFIER_1"/>
0073	</ResponsePayload>
0074	</BatchItem>
0075	</ResponseMessage>
0069	# TIME 1
0070	<RequestMessage>
0071	<RequestHeader>
0072	<ProtocolVersion>
0073	<ProtocolVersionMajor type="Integer" value="1"/>
0074	<ProtocolVersionMinor type="Integer" value="1"/>
0075	</ProtocolVersion>
	<BatchCount type="Integer" value="1"/>



```

0076 </RequestHeader>
0077 <BatchItem>
0078   <Operation type="Enumeration" value="GetAttributes"/>
0079   <RequestPayload>
0080     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0081     <AttributeName type="TextString" value="State"/>
0082     <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0083     <AttributeName type="TextString" value="Unique Identifier"/>
0084     <AttributeName type="TextString" value="Object Type"/>
0085     <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0086     <AttributeName type="TextString" value="Cryptographic
Length"/>
0087     <AttributeName type="TextString" value="Digest"/>
0088     <AttributeName type="TextString" value="Initial Date"/>
0089     <AttributeName type="TextString" value="Last Change Date"/>
0090     <AttributeName type="TextString" value="Activation Date"/>
0091   </RequestPayload>
0092 </BatchItem>
0093 </RequestMessage>
0094 <ResponseMessage>
0095   <ResponseHeader>
0096     <ProtocolVersion>
0097       <ProtocolVersionMajor type="Integer" value="1"/>
0098       <ProtocolVersionMinor type="Integer" value="1"/>
0099     </ProtocolVersion>
0100     <TimeStamp type="DateTime" value="2012-04-27T08:12:24+00:00"/>
0101     <BatchCount type="Integer" value="1"/>
0102   </ResponseHeader>
0103   <BatchItem>
0104     <Operation type="Enumeration" value="GetAttributes"/>
0105     <ResultStatus type="Enumeration" value="Success"/>
0106     <ResponsePayload>
0107       <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0108       <Attribute>
0109         <AttributeName type="TextString" value="State"/>
0110         <AttributeValue type="Enumeration" value="PreActive"/>
0111       </Attribute>
0112       <Attribute>
0113         <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0114         <AttributeValue type="Integer" value="Sign"/>
0115       </Attribute>
0116       <Attribute>
0117         <AttributeName type="TextString" value="Unique Identifier"/>
0118         <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0119       </Attribute>
0120       <Attribute>
0121         <AttributeName type="TextString" value="Object Type"/>
0122         <AttributeValue type="Enumeration" value="PrivateKey"/>
0123       </Attribute>
0124       <Attribute>
0125         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>

```

0126	<AttributeValue type="Enumeration" value="RSA"/>
0127	</Attribute>
0128	<Attribute>
0129	<AttributeName type="TextString" value="Cryptographic Length"/>
0130	<AttributeValue type="Integer" value="2048"/>
0131	</Attribute>
0132	<Attribute>
0133	<AttributeName type="TextString" value="Digest"/>
0134	<AttributeValue>
0135	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0136	<DigestValue type="ByteString" value="8eb422ae2b006a05d3c8a542a28536735241b6dc1c37926bc8007bd6220d9230"/>
0137	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0138	</AttributeValue>
0139	</Attribute>
0140	<Attribute>
0141	<AttributeName type="TextString" value="Initial Date"/>
0142	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0143	</Attribute>
0144	<Attribute>
0145	<AttributeName type="TextString" value="Last Change Date"/>
0146	<AttributeValue type="DateTime" value="2013-01-11T08:18:21+00:00"/>
0147	</Attribute>
0148	</ResponsePayload>
0149	</BatchItem>
0150	</ResponseMessage>
0151	# TIME 2 <RequestMessage>
0152	<RequestHeader>
0153	<ProtocolVersion>
0154	<ProtocolVersionMajor type="Integer" value="1"/>
0155	<ProtocolVersionMinor type="Integer" value="1"/>
0156	</ProtocolVersion>
0157	<BatchCount type="Integer" value="1"/>
0158	</RequestHeader>
0159	<BatchItem>
0160	<Operation type="Enumeration" value="Destroy"/>
0161	<RequestPayload>
0162	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0163	</RequestPayload>
0164	</BatchItem>
0165	</RequestMessage>
0166	<ResponseMessage>
0167	<ResponseHeader>
0168	<ProtocolVersion>
0169	<ProtocolVersionMajor type="Integer" value="1"/>
0170	<ProtocolVersionMinor type="Integer" value="1"/>
0171	</ProtocolVersion>
0172	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0173	<BatchCount type="Integer" value="1"/>
0174	</ResponseHeader>
0175	<BatchItem>
0176	<Operation type="Enumeration" value="Destroy"/>

0177	<ResponseStatus type="Enumeration" value="Success"/>
0178	<ResponsePayload>
0179	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0180	</ResponsePayload>
0181	</BatchItem>
0182	</ResponseMessage>
	# TIME 3
0183	<RequestMessage>
0184	<RequestHeader>
0185	<ProtocolVersion>
0186	<ProtocolVersionMajor type="Integer" value="1"/>
0187	<ProtocolVersionMinor type="Integer" value="1"/>
0188	</ProtocolVersion>
0189	<BatchCount type="Integer" value="1"/>
0190	</RequestHeader>
0191	<BatchItem>
0192	<Operation type="Enumeration" value="GetAttributes"/>
0193	<RequestPayload>
0194	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0195	</RequestPayload>
0196	</BatchItem>
0197	</RequestMessage>
0198	<ResponseMessage>
0199	<ResponseHeader>
0200	<ProtocolVersion>
0201	<ProtocolVersionMajor type="Integer" value="1"/>
0202	<ProtocolVersionMinor type="Integer" value="1"/>
0203	</ProtocolVersion>
0204	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0205	<BatchCount type="Integer" value="1"/>
0206	</ResponseHeader>
0207	<BatchItem>
0208	<Operation type="Enumeration" value="GetAttributes"/>
0209	<ResponseStatus type="Enumeration" value="Success"/>
0210	<ResponsePayload>
0211	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0212	<Attribute>
0213	<AttributeName type="TextString" value="Unique Identifier"/>
0214	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0215	</Attribute>
0216	<Attribute>
0217	<AttributeName type="TextString" value="Object Type"/>
0218	<AttributeValue type="Enumeration" value="PrivateKey"/>
0219	</Attribute>
0220	<Attribute>
0221	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0222	<AttributeValue type="Enumeration" value="RSA"/>
0223	</Attribute>
0224	<Attribute>
0225	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0226	<AttributeValue type="Integer" value="2048"/>
0227	</Attribute>

```

0228     <Attribute>
0229     <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0230     <AttributeValue type="Integer" value="Sign"/>
0231     </Attribute>
0232     <Attribute>
0233     <AttributeName type="TextString" value="Destroy Date"/>
0234     <AttributeValue type="DateTime" value="2013-01-
11T08:40:05+00:00"/>
0235     </Attribute>
0236     <Attribute>
0237     <AttributeName type="TextString" value="Digest"/>
0238     <AttributeValue>
0239     <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0240     <DigestValue type="ByteString"
value="4abc48c2ba00a6bba22cb6fc2827b46107354968872b395edb31354e78878
be6"/>
0241     <KeyFormatType type="Enumeration" value="PKCS_1"/>
0242     </AttributeValue>
0243     </Attribute>
0244     <Attribute>
0245     <AttributeName type="TextString" value="Fresh"/>
0246     <AttributeValue type="Boolean" value="true"/>
0247     </Attribute>
0248     <Attribute>
0249     <AttributeName type="TextString" value="Initial Date"/>
0250     <AttributeValue type="DateTime" value="2013-01-
11T08:40:05+00:00"/>
0251     </Attribute>
0252     <Attribute>
0253     <AttributeName type="TextString" value="Last Change Date"/>
0254     <AttributeValue type="DateTime" value="2013-01-
11T08:40:05+00:00"/>
0255     </Attribute>
0256     <Attribute>
0257     <AttributeName type="TextString" value="Lease Time"/>
0258     <AttributeValue type="Interval" value="3600"/>
0259     </Attribute>
0260     <Attribute>
0261     <AttributeName type="TextString" value="Link"/>
0262     <AttributeValue>
0263     <LinkType type="Enumeration" value="PublicKeyLink"/>
0264     <LinkedObjectIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0265     </AttributeValue>
0266     </Attribute>
0267     <Attribute>
0268     <AttributeName type="TextString" value="Name"/>
0269     <AttributeValue>
0270     <NameValue type="TextString" value="AKLC-O-1-11-private"/>
0271     <NameType type="Enumeration"
value="UninterpretedTextString"/>
0272     </AttributeValue>
0273     </Attribute>
0274     <Attribute>
0275     <AttributeName type="TextString" value="State"/>
0276     <AttributeValue type="Enumeration" value="Destroyed"/>
0277     </Attribute>

```

0278	</ResponsePayload>
0279	</BatchItem>
0280	</ResponseMessage>
0281	# TIME 4 <RequestMessage>
0282	<RequestHeader>
0283	<ProtocolVersion>
0284	<ProtocolVersionMajor type="Integer" value="1"/>
0285	<ProtocolVersionMinor type="Integer" value="1"/>
0286	</ProtocolVersion>
0287	<BatchCount type="Integer" value="1"/>
0288	</RequestHeader>
0289	<BatchItem>
0290	<Operation type="Enumeration" value="GetAttributes"/>
0291	<RequestPayload>
0292	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0293	</RequestPayload>
0294	</BatchItem>
0295	</RequestMessage>
0296	<ResponseMessage>
0297	<ResponseHeader>
0298	<ProtocolVersion>
0299	<ProtocolVersionMajor type="Integer" value="1"/>
0300	<ProtocolVersionMinor type="Integer" value="1"/>
0301	</ProtocolVersion>
0302	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0303	<BatchCount type="Integer" value="1"/>
0304	</ResponseHeader>
0305	<BatchItem>
0306	<Operation type="Enumeration" value="GetAttributes"/>
0307	<ResultStatus type="Enumeration" value="Success"/>
0308	<ResponsePayload>
0309	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0310	<Attribute>
0311	<AttributeName type="TextString" value="Unique Identifier"/>
0312	<AttributeValue type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0313	</Attribute>
0314	<Attribute>
0315	<AttributeName type="TextString" value="Object Type"/>
0316	<AttributeValue type="Enumeration" value="PublicKey"/>
0317	</Attribute>
0318	<Attribute>
0319	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0320	<AttributeValue type="Enumeration" value="RSA"/>
0321	</Attribute>
0322	<Attribute>
0323	<AttributeName type="TextString" value="Cryptographic Length"/>
0324	<AttributeValue type="Integer" value="2048"/>
0325	</Attribute>
0326	<Attribute>
0327	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0328	<AttributeValue type="Integer" value="Verify"/>

0329	</Attribute>
0330	<Attribute>
0331	<AttributeName type="TextString" value="Digest"/>
0332	<AttributeValue>
0333	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0334	<DigestValue type="ByteString" value="330306b0e337e32dd1b5acf92cb96fd39adb802f305e7406062248324816f445"/>
0335	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0336	</AttributeValue>
0337	</Attribute>
0338	<Attribute>
0339	<AttributeName type="TextString" value="Fresh"/>
0340	<AttributeValue type="Boolean" value="true"/>
0341	</Attribute>
0342	<Attribute>
0343	<AttributeName type="TextString" value="Initial Date"/>
0344	<AttributeValue type="DateTime" value="2013-01-11T08:37:43+00:00"/>
0345	</Attribute>
0346	<Attribute>
0347	<AttributeName type="TextString" value="Last Change Date"/>
0348	<AttributeValue type="DateTime" value="2013-01-11T08:37:43+00:00"/>
0349	</Attribute>
0350	<Attribute>
0351	<AttributeName type="TextString" value="Lease Time"/>
0352	<AttributeValue type="Interval" value="3600"/>
0353	</Attribute>
0354	<Attribute>
0355	<AttributeName type="TextString" value="Link"/>
0356	<AttributeValue>
0357	<LinkType type="Enumeration" value="PrivateKeyLink"/>
0358	<LinkedObjectIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0359	</AttributeValue>
0360	</Attribute>
0361	<Attribute>
0362	<AttributeName type="TextString" value="Name"/>
0363	<AttributeValue>
0364	<NameValue type="TextString" value="AKLC-O-1-11-public"/>
0365	<NameType type="Enumeration" value="UninterpretedTextString"/>
0366	</AttributeValue>
0367	</Attribute>
0368	<Attribute>
0369	<AttributeName type="TextString" value="State"/>
0370	<AttributeValue type="Enumeration" value="PreActive"/>
0371	</Attribute>
0372	</ResponsePayload>
0373	</BatchItem>
0374	</ResponseMessage>
	# TIME 5
0375	<RequestMessage>
0376	<RequestHeader>
0377	<ProtocolVersion>
0378	<ProtocolVersionMajor type="Integer" value="1"/>
0379	<ProtocolVersionMinor type="Integer" value="1"/>

0380	</ProtocolVersion>
0381	<BatchCount type="Integer" value="1"/>
0382	</RequestHeader>
0383	<BatchItem>
0384	<Operation type="Enumeration" value="Destroy"/>
0385	<RequestPayload>
0386	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0387	</RequestPayload>
0388	</BatchItem>
0389	</RequestMessage>
0390	<ResponseMessage>
0391	<ResponseHeader>
0392	<ProtocolVersion>
0393	<ProtocolVersionMajor type="Integer" value="1"/>
0394	<ProtocolVersionMinor type="Integer" value="1"/>
0395	</ProtocolVersion>
0396	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0397	<BatchCount type="Integer" value="1"/>
0398	</ResponseHeader>
0399	<BatchItem>
0400	<Operation type="Enumeration" value="Destroy"/>
0401	<ResultStatus type="Enumeration" value="Success"/>
0402	<ResponsePayload>
0403	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0404	</ResponsePayload>
0405	</BatchItem>
0406	</ResponseMessage>
0407	<i># TIME 6</i> <RequestMessage>
0408	<RequestHeader>
0409	<ProtocolVersion>
0410	<ProtocolVersionMajor type="Integer" value="1"/>
0411	<ProtocolVersionMinor type="Integer" value="1"/>
0412	</ProtocolVersion>
0413	<BatchCount type="Integer" value="1"/>
0414	</RequestHeader>
0415	<BatchItem>
0416	<Operation type="Enumeration" value="GetAttributes"/>
0417	<RequestPayload>
0418	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0419	</RequestPayload>
0420	</BatchItem>
0421	</RequestMessage>
0422	<ResponseMessage>
0423	<ResponseHeader>
0424	<ProtocolVersion>
0425	<ProtocolVersionMajor type="Integer" value="1"/>
0426	<ProtocolVersionMinor type="Integer" value="1"/>
0427	</ProtocolVersion>
0428	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0429	<BatchCount type="Integer" value="1"/>
0430	</ResponseHeader>
0431	<BatchItem>
0432	<Operation type="Enumeration" value="GetAttributes"/>
0433	<ResultStatus type="Enumeration" value="Success"/>

```

0434     <ResponsePayload>
0435     <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0436     <Attribute>
0437         <AttributeName type="TextString" value="Unique Identifier"/>
0438         <AttributeValue type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0439     </Attribute>
0440     <Attribute>
0441         <AttributeName type="TextString" value="Object Type"/>
0442         <AttributeValue type="Enumeration" value="PublicKey"/>
0443     </Attribute>
0444     <Attribute>
0445         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0446         <AttributeValue type="Enumeration" value="RSA"/>
0447     </Attribute>
0448     <Attribute>
0449         <AttributeName type="TextString" value="Cryptographic
Length"/>
0450         <AttributeValue type="Integer" value="2048"/>
0451     </Attribute>
0452     <Attribute>
0453         <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0454         <AttributeValue type="Integer" value="Verify"/>
0455     </Attribute>
0456     <Attribute>
0457         <AttributeName type="TextString" value="Destroy Date"/>
0458         <AttributeValue type="DateTime" value="2013-01-
11T08:38:18+00:00"/>
0459     </Attribute>
0460     <Attribute>
0461         <AttributeName type="TextString" value="Digest"/>
0462         <AttributeValue>
0463             <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0464             <DigestValue type="ByteString"
value="b06f3e3d107a282adb5fe316356d13679d7cf7429d14a6f20665f45ba4d28
83c"/>
0465         <KeyFormatType type="Enumeration" value="PKCS_1"/>
0466     </AttributeValue>
0467     </Attribute>
0468     <Attribute>
0469         <AttributeName type="TextString" value="Fresh"/>
0470         <AttributeValue type="Boolean" value="true"/>
0471     </Attribute>
0472     <Attribute>
0473         <AttributeName type="TextString" value="Initial Date"/>
0474         <AttributeValue type="DateTime" value="2013-01-
11T08:38:18+00:00"/>
0475     </Attribute>
0476     <Attribute>
0477         <AttributeName type="TextString" value="Last Change Date"/>
0478         <AttributeValue type="DateTime" value="2013-01-
11T08:38:18+00:00"/>
0479     </Attribute>
0480     <Attribute>
0481         <AttributeName type="TextString" value="Lease Time"/>

```



```

0482     <AttributeValue type="Interval" value="3600"/>
0483     </Attribute>
0484     <Attribute>
0485         <AttributeName type="TextString" value="Link"/>
0486         <AttributeValue>
0487             <LinkType type="Enumeration" value="PrivateKeyLink"/>
0488             <LinkedObjectIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0489         </AttributeValue>
0490     </Attribute>
0491     <Attribute>
0492         <AttributeName type="TextString" value="Name"/>
0493         <AttributeValue>
0494             <NameValue type="TextString" value="AKLC-O-1-11-public"/>
0495             <NameType type="Enumeration"
value="UninterpretedTextString"/>
0496         </AttributeValue>
0497     </Attribute>
0498     <Attribute>
0499         <AttributeName type="TextString" value="State"/>
0500         <AttributeValue type="Enumeration" value="Destroyed"/>
0501     </Attribute>
0502 </ResponsePayload>
0503 </BatchItem>
0504 </ResponseMessage>

```

138

## 139 3.6 Optional Test Cases KMIP v1.2

### 140 3.6.1 AKLC-O-1-12

141 CreateKeyPair, 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="CreateKeyPair"/>
0011     <RequestPayload>
0012       <CommonTemplateAttribute>
0013         <Attribute>
0014           <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0015           <AttributeValue type="Enumeration" value="RSA"/>
0016         </Attribute>
0017         <Attribute>
0018           <AttributeName type="TextString" value="Cryptographic
Length"/>
0019           <AttributeValue type="Integer" value="2048"/>
0020         </Attribute>
0021       </CommonTemplateAttribute>
0022     <PrivateKeyTemplateAttribute>

```

0023	<Attribute>
0024	<AttributeName type="TextString" value="Name"/>
0025	<AttributeValue>
0026	<NameValue type="TextString" value="AKLC-O-1-12-private"/>
0027	<NameType type="Enumeration" value="UninterpretedTextString"/>
0028	</AttributeValue>
0029	</Attribute>
0030	<Attribute>
0031	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0032	<AttributeValue type="Integer" value="Sign"/>
0033	</Attribute>
0034	</PrivateKeyTemplateAttribute>
0035	<PublicKeyTemplateAttribute>
0036	<Attribute>
0037	<AttributeName type="TextString" value="Name"/>
0038	<AttributeValue>
0039	<NameValue type="TextString" value="AKLC-O-1-12-public"/>
0040	<NameType type="Enumeration" value="UninterpretedTextString"/>
0041	</AttributeValue>
0042	</Attribute>
0043	<Attribute>
0044	<AttributeName type="TextString" value="Cryptographic Usage Mask"/>
0045	<AttributeValue type="Integer" value="Verify"/>
0046	</Attribute>
0047	</PublicKeyTemplateAttribute>
0048	</RequestPayload>
0049	</BatchItem>
0050	</RequestMessage>
0051	<ResponseMessage>
0052	<ResponseHeader>
0053	<ProtocolVersion>
0054	<ProtocolVersionMajor type="Integer" value="1"/>
0055	<ProtocolVersionMinor type="Integer" value="2"/>
0056	</ProtocolVersion>
0057	<TimeStamp type="DateTime" value="2013-01-11T08:32:04+00:00"/>
0058	<BatchCount type="Integer" value="1"/>
0059	</ResponseHeader>
0060	<BatchItem>
0061	<Operation type="Enumeration" value="CreateKeyPair"/>
0062	<ResultStatus type="Enumeration" value="Success"/>
0063	<ResponsePayload>
0064	<PrivateKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0065	<PublicKeyUniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0066	</ResponsePayload>
0067	</BatchItem>
0068	</ResponseMessage>
0069	# TIME 1 <RequestMessage>
0070	<RequestHeader>
0071	<ProtocolVersion>

```

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

```

0122	<AttributeName type="TextString" value="Object Type"/>
0123	<AttributeValue type="Enumeration" value="PrivateKey"/>
0124	</Attribute>
0125	<Attribute>
0126	<AttributeName type="TextString" value="Cryptographic Algorithm"/>
0127	<AttributeValue type="Enumeration" value="RSA"/>
0128	</Attribute>
0129	<Attribute>
0130	<AttributeName type="TextString" value="Cryptographic Length"/>
0131	<AttributeValue type="Integer" value="2048"/>
0132	</Attribute>
0133	<Attribute>
0134	<AttributeName type="TextString" value="Digest"/>
0135	<AttributeValue>
0136	<HashingAlgorithm type="Enumeration" value="SHA_256"/>
0137	<DigestValue type="ByteString" value="8eb422ae2b006a05d3c8a542a28536735241b6dc1c37926bc8007bd6220d9 230"/>
0138	<KeyFormatType type="Enumeration" value="PKCS_1"/>
0139	</AttributeValue>
0140	</Attribute>
0141	<Attribute>
0142	<AttributeName type="TextString" value="Initial Date"/>
0143	<AttributeValue type="DateTime" value="2013-01- 11T08:18:21+00:00"/>
0144	</Attribute>
0145	<Attribute>
0146	<AttributeName type="TextString" value="Last Change Date"/>
0147	<AttributeValue type="DateTime" value="2013-01- 11T08:18:21+00:00"/>
0148	</Attribute>
0149	<Attribute>
0150	<AttributeName type="TextString" value="Original Creation Date"/>
0151	<AttributeValue type="DateTime" value="2013-01- 11T08:18:21+00:00"/>
0152	</Attribute>
0153	</ResponsePayload>
0154	</BatchItem>
0155	</ResponseMessage>
	<i># TIME 2</i>
0156	<RequestMessage>
0157	<RequestHeader>
0158	<ProtocolVersion>
0159	<ProtocolVersionMajor type="Integer" value="1"/>
0160	<ProtocolVersionMinor type="Integer" value="2"/>
0161	</ProtocolVersion>
0162	<BatchCount type="Integer" value="1"/>
0163	</RequestHeader>
0164	<BatchItem>
0165	<Operation type="Enumeration" value="Destroy"/>
0166	<RequestPayload>
0167	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0168	</RequestPayload>
0169	</BatchItem>

0170	</RequestMessage>
0171	<ResponseMessage>
0172	<ResponseHeader>
0173	<ProtocolVersion>
0174	<ProtocolVersionMajor type="Integer" value="1"/>
0175	<ProtocolVersionMinor type="Integer" value="2"/>
0176	</ProtocolVersion>
0177	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0178	<BatchCount type="Integer" value="1"/>
0179	</ResponseHeader>
0180	<BatchItem>
0181	<Operation type="Enumeration" value="Destroy"/>
0182	<ResultStatus type="Enumeration" value="Success"/>
0183	<ResponsePayload>
0184	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0185	</ResponsePayload>
0186	</BatchItem>
0187	</ResponseMessage>
	<i># TIME 3</i>
0188	<RequestMessage>
0189	<RequestHeader>
0190	<ProtocolVersion>
0191	<ProtocolVersionMajor type="Integer" value="1"/>
0192	<ProtocolVersionMinor type="Integer" value="2"/>
0193	</ProtocolVersion>
0194	<BatchCount type="Integer" value="1"/>
0195	</RequestHeader>
0196	<BatchItem>
0197	<Operation type="Enumeration" value="GetAttributes"/>
0198	<RequestPayload>
0199	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0200	</RequestPayload>
0201	</BatchItem>
0202	</RequestMessage>
0203	<ResponseMessage>
0204	<ResponseHeader>
0205	<ProtocolVersion>
0206	<ProtocolVersionMajor type="Integer" value="1"/>
0207	<ProtocolVersionMinor type="Integer" value="2"/>
0208	</ProtocolVersion>
0209	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0210	<BatchCount type="Integer" value="1"/>
0211	</ResponseHeader>
0212	<BatchItem>
0213	<Operation type="Enumeration" value="GetAttributes"/>
0214	<ResultStatus type="Enumeration" value="Success"/>
0215	<ResponsePayload>
0216	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0217	<Attribute>
0218	<AttributeName type="TextString" value="Unique Identifier"/>
0219	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0220	</Attribute>
0221	<Attribute>
0222	<AttributeName type="TextString" value="Object Type"/>

```

0223     <AttributeValue type="Enumeration" value="PrivateKey"/>
0224     </Attribute>
0225     <Attribute>
0226     <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0227     <AttributeValue type="Enumeration" value="RSA"/>
0228     </Attribute>
0229     <Attribute>
0230     <AttributeName type="TextString" value="Cryptographic
Length"/>
0231     <AttributeValue type="Integer" value="2048"/>
0232     </Attribute>
0233     <Attribute>
0234     <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0235     <AttributeValue type="Integer" value="Sign"/>
0236     </Attribute>
0237     <Attribute>
0238     <AttributeName type="TextString" value="Destroy Date"/>
0239     <AttributeValue type="DateTime" value="2013-01-
11T08:40:05+00:00"/>
0240     </Attribute>
0241     <Attribute>
0242     <AttributeName type="TextString" value="Digest"/>
0243     <AttributeValue>
0244     <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0245     <DigestValue type="ByteString"
value="4abc48c2ba00a6bba22cb6fc2827b46107354968872b395edb31354e78878
be6"/>
0246     <KeyFormatType type="Enumeration" value="PKCS_1"/>
0247     </AttributeValue>
0248     </Attribute>
0249     <Attribute>
0250     <AttributeName type="TextString" value="Fresh"/>
0251     <AttributeValue type="Boolean" value="true"/>
0252     </Attribute>
0253     <Attribute>
0254     <AttributeName type="TextString" value="Initial Date"/>
0255     <AttributeValue type="DateTime" value="2013-01-
11T08:40:05+00:00"/>
0256     </Attribute>
0257     <Attribute>
0258     <AttributeName type="TextString" value="Last Change Date"/>
0259     <AttributeValue type="DateTime" value="2013-01-
11T08:40:05+00:00"/>
0260     </Attribute>
0261     <Attribute>
0262     <AttributeName type="TextString" value="Lease Time"/>
0263     <AttributeValue type="Interval" value="3600"/>
0264     </Attribute>
0265     <Attribute>
0266     <AttributeName type="TextString" value="Link"/>
0267     <AttributeValue>
0268     <LinkType type="Enumeration" value="PublicKeyLink"/>
0269     <LinkedObjectIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
0270     </AttributeValue>
0271     </Attribute>

```

0272	<Attribute>
0273	<AttributeName type="TextString" value="Name"/>
0274	<AttributeValue>
0275	<NameValue type="TextString" value="AKLC-O-1-12-private"/>
0276	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0277	</AttributeValue>
0278	</Attribute>
0279	<Attribute>
0280	<AttributeName type="TextString" value="Original Creation
	Date"/>
0281	<AttributeValue type="DateTime" value="2013-01-
	11T08:40:05+00:00"/>
0282	</Attribute>
0283	<Attribute>
0284	<AttributeName type="TextString" value="State"/>
0285	<AttributeValue type="Enumeration" value="Destroyed"/>
0286	</Attribute>
0287	</ResponsePayload>
0288	</BatchItem>
0289	</ResponseMessage>
	# TIME 4
0290	<RequestMessage>
0291	<RequestHeader>
0292	<ProtocolVersion>
0293	<ProtocolVersionMajor type="Integer" value="1"/>
0294	<ProtocolVersionMinor type="Integer" value="2"/>
0295	</ProtocolVersion>
0296	<BatchCount type="Integer" value="1"/>
0297	</RequestHeader>
0298	<BatchItem>
0299	<Operation type="Enumeration" value="GetAttributes"/>
0300	<RequestPayload>
0301	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0302	</RequestPayload>
0303	</BatchItem>
0304	</RequestMessage>
0305	<ResponseMessage>
0306	<ResponseHeader>
0307	<ProtocolVersion>
0308	<ProtocolVersionMajor type="Integer" value="1"/>
0309	<ProtocolVersionMinor type="Integer" value="2"/>
0310	</ProtocolVersion>
0311	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0312	<BatchCount type="Integer" value="1"/>
0313	</ResponseHeader>
0314	<BatchItem>
0315	<Operation type="Enumeration" value="GetAttributes"/>
0316	<ResultStatus type="Enumeration" value="Success"/>
0317	<ResponsePayload>
0318	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0319	<Attribute>
0320	<AttributeName type="TextString" value="Unique Identifier"/>
0321	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0322	</Attribute>

```

0323     <Attribute>
0324         <AttributeName type="TextString" value="Object Type"/>
0325         <AttributeValue type="Enumeration" value="PublicKey"/>
0326     </Attribute>
0327     <Attribute>
0328         <AttributeName type="TextString" value="Cryptographic
Algorithm"/>
0329         <AttributeValue type="Enumeration" value="RSA"/>
0330     </Attribute>
0331     <Attribute>
0332         <AttributeName type="TextString" value="Cryptographic
Length"/>
0333         <AttributeValue type="Integer" value="2048"/>
0334     </Attribute>
0335     <Attribute>
0336         <AttributeName type="TextString" value="Cryptographic Usage
Mask"/>
0337         <AttributeValue type="Integer" value="Verify"/>
0338     </Attribute>
0339     <Attribute>
0340         <AttributeName type="TextString" value="Digest"/>
0341         <AttributeValue>
0342             <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0343             <DigestValue type="ByteString"
value="330306b0e337e32ddb5acf92cb96fd39adb802f305e7406062248324816f
445"/>
0344         <KeyFormatType type="Enumeration" value="PKCS_1"/>
0345     </AttributeValue>
0346 </Attribute>
0347 <Attribute>
0348     <AttributeName type="TextString" value="Fresh"/>
0349     <AttributeValue type="Boolean" value="true"/>
0350 </Attribute>
0351 <Attribute>
0352     <AttributeName type="TextString" value="Initial Date"/>
0353     <AttributeValue type="DateTime" value="2013-01-
11T08:37:43+00:00"/>
0354 </Attribute>
0355 <Attribute>
0356     <AttributeName type="TextString" value="Last Change Date"/>
0357     <AttributeValue type="DateTime" value="2013-01-
11T08:37:43+00:00"/>
0358 </Attribute>
0359 <Attribute>
0360     <AttributeName type="TextString" value="Lease Time"/>
0361     <AttributeValue type="Interval" value="3600"/>
0362 </Attribute>
0363 <Attribute>
0364     <AttributeName type="TextString" value="Link"/>
0365     <AttributeValue>
0366         <LinkType type="Enumeration" value="PrivateKeyLink"/>
0367         <LinkedObjectIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0368     </AttributeValue>
0369 </Attribute>
0370 <Attribute>
0371     <AttributeName type="TextString" value="Name"/>
0372     <AttributeValue>

```



0373	<NameValue type="TextString" value="AKLC-O-1-12-public"/>
0374	<NameType type="Enumeration" value="UninterpretedTextString"/>
0375	</AttributeValue>
0376	</Attribute>
0377	<Attribute>
0378	<AttributeName type="TextString" value="Original Creation Date"/>
0379	<AttributeValue type="DateTime" value="2013-01-11T08:37:43+00:00"/>
0380	</Attribute>
0381	<Attribute>
0382	<AttributeName type="TextString" value="State"/>
0383	<AttributeValue type="Enumeration" value="PreActive"/>
0384	</Attribute>
0385	</ResponsePayload>
0386	</BatchItem>
0387	</ResponseMessage>
0388	# TIME 5 <RequestMessage>
0389	<RequestHeader>
0390	<ProtocolVersion>
0391	<ProtocolVersionMajor type="Integer" value="1"/>
0392	<ProtocolVersionMinor type="Integer" value="2"/>
0393	</ProtocolVersion>
0394	<BatchCount type="Integer" value="1"/>
0395	</RequestHeader>
0396	<BatchItem>
0397	<Operation type="Enumeration" value="Destroy"/>
0398	<RequestPayload>
0399	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0400	</RequestPayload>
0401	</BatchItem>
0402	</RequestMessage>
0403	<ResponseMessage>
0404	<ResponseHeader>
0405	<ProtocolVersion>
0406	<ProtocolVersionMajor type="Integer" value="1"/>
0407	<ProtocolVersionMinor type="Integer" value="2"/>
0408	</ProtocolVersion>
0409	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0410	<BatchCount type="Integer" value="1"/>
0411	</ResponseHeader>
0412	<BatchItem>
0413	<Operation type="Enumeration" value="Destroy"/>
0414	<ResultStatus type="Enumeration" value="Success"/>
0415	<ResponsePayload>
0416	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0417	</ResponsePayload>
0418	</BatchItem>
0419	</ResponseMessage>
0420	# TIME 6 <RequestMessage>
0421	<RequestHeader>
0422	<ProtocolVersion>
0423	<ProtocolVersionMajor type="Integer" value="1"/>

0424	<ProtocolVersionMinor type="Integer" value="2"/>
0425	</ProtocolVersion>
0426	<BatchCount type="Integer" value="1"/>
0427	</RequestHeader>
0428	<BatchItem>
0429	<Operation type="Enumeration" value="GetAttributes"/>
0430	<RequestPayload>
0431	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0432	</RequestPayload>
0433	</BatchItem>
0434	</RequestMessage>
0435	<ResponseMessage>
0436	<ResponseHeader>
0437	<ProtocolVersion>
0438	<ProtocolVersionMajor type="Integer" value="1"/>
0439	<ProtocolVersionMinor type="Integer" value="2"/>
0440	</ProtocolVersion>
0441	<TimeStamp type="DateTime" value="2012-04-27T08:12:25+00:00"/>
0442	<BatchCount type="Integer" value="1"/>
0443	</ResponseHeader>
0444	<BatchItem>
0445	<Operation type="Enumeration" value="GetAttributes"/>
0446	<ResultStatus type="Enumeration" value="Success"/>
0447	<ResponsePayload>
0448	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0449	<Attribute>
0450	<AttributeName type="TextString" value="Unique Identifier"/>
0451	<AttributeValue type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0452	</Attribute>
0453	<Attribute>
0454	<AttributeName type="TextString" value="Object Type"/>
0455	<AttributeValue type="Enumeration" value="PublicKey"/>
0456	</Attribute>
0457	<Attribute>
0458	<AttributeName type="TextString" value="Cryptographic
	Algorithm"/>
0459	<AttributeValue type="Enumeration" value="RSA"/>
0460	</Attribute>
0461	<Attribute>
0462	<AttributeName type="TextString" value="Cryptographic
	Length"/>
0463	<AttributeValue type="Integer" value="2048"/>
0464	</Attribute>
0465	<Attribute>
0466	<AttributeName type="TextString" value="Cryptographic Usage
	Mask"/>
0467	<AttributeValue type="Integer" value="Verify"/>
0468	</Attribute>
0469	<Attribute>
0470	<AttributeName type="TextString" value="Destroy Date"/>
0471	<AttributeValue type="DateTime" value="2013-01-
	11T08:38:18+00:00"/>
0472	</Attribute>
0473	<Attribute>
0474	<AttributeName type="TextString" value="Digest"/>

```

0475     <AttributeValue>
0476     <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0477     <DigestValue type="ByteString"
value="b06f3e3d107a282adb5fe316356d13679d7cf7429d14a6f20665f45ba4d28
83c"/>
0478     <KeyFormatType type="Enumeration" value="PKCS_1"/>
0479     </AttributeValue>
0480     </Attribute>
0481     <Attribute>
0482     <AttributeName type="TextString" value="Fresh"/>
0483     <AttributeValue type="Boolean" value="true"/>
0484     </Attribute>
0485     <Attribute>
0486     <AttributeName type="TextString" value="Initial Date"/>
0487     <AttributeValue type="DateTime" value="2013-01-
11T08:38:18+00:00"/>
0488     </Attribute>
0489     <Attribute>
0490     <AttributeName type="TextString" value="Last Change Date"/>
0491     <AttributeValue type="DateTime" value="2013-01-
11T08:38:18+00:00"/>
0492     </Attribute>
0493     <Attribute>
0494     <AttributeName type="TextString" value="Lease Time"/>
0495     <AttributeValue type="Interval" value="3600"/>
0496     </Attribute>
0497     <Attribute>
0498     <AttributeName type="TextString" value="Link"/>
0499     <AttributeValue>
0500     <LinkType type="Enumeration" value="PrivateKeyLink"/>
0501     <LinkedObjectIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0502     </AttributeValue>
0503     </Attribute>
0504     <Attribute>
0505     <AttributeName type="TextString" value="Name"/>
0506     <AttributeValue>
0507     <NameValue type="TextString" value="AKLC-O-1-12-public"/>
0508     <NameType type="Enumeration"
value="UninterpretedTextString"/>
0509     </AttributeValue>
0510     </Attribute>
0511     <Attribute>
0512     <AttributeName type="TextString" value="Original Creation
Date"/>
0513     <AttributeValue type="DateTime" value="2013-01-
11T08:37:43+00:00"/>
0514     </Attribute>
0515     <Attribute>
0516     <AttributeName type="TextString" value="State"/>
0517     <AttributeValue type="Enumeration" value="Destroyed"/>
0518     </Attribute>
0519     </ResponsePayload>
0520     </BatchItem>
0521     </ResponseMessage>

```

---

## 143 4 Conformance

### 144 4.1 Asymmetric Key Lifecycle Client KMIP v1.0 Profile Conformance

145 KMIP client implementations conformant to this profile:

- 146 1. SHALL support the Authentication Suite conditions (2.1) and;
- 147 2. SHALL support the **Error! Reference source not found.** conditions (**Error! Reference source**
- 148 **not found.**) and;
- 149 3. SHALL support all Mandatory Test Cases KMIP v1.0 (3.1)

### 150 4.2 Asymmetric Key Lifecycle Client KMIP v1.1 Profile Conformance

151 KMIP client implementations conformant to this profile:

- 152 1. SHALL support the Authentication Suite conditions (2.1) and;
- 153 2. SHALL support the **Error! Reference source not found.** conditions (**Error! Reference source**
- 154 **not found.**) and;
- 155 3. SHALL support all Mandatory Test Cases KMIP v1.1 (3.2)

### 156 4.3 Asymmetric Key Lifecycle Client KMIP v1.2 Profile Conformance

157 KMIP client implementations conformant to this profile:

- 158 1. SHALL support the Authentication Suite conditions (2.1) and;
- 159 2. SHALL support the **Error! Reference source not found.** conditions (**Error! Reference source**
- 160 **not found.**) and;
- 161 3. SHALL support all Mandatory Test Cases KMIP v1.2 (3.3)

### 162 4.4 Asymmetric Key Lifecycle Client KMIP v1.0 Profile Conformance

163 KMIP server implementations conformant to this profile:

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

### 167 4.5 Asymmetric Key Lifecycle Client KMIP v1.1 Profile Conformance

168 KMIP server implementations conformant to this profile:

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

### 172 4.6 Asymmetric Key Lifecycle Client KMIP v1.2 Profile Conformance

173 KMIP server implementations conformant to this profile:

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

## 177 4.7 Permitted Test Case Variations

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

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

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

### 183 4.7.1 Variable Items

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

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

- 220 a. The HashingAlgorithm selected by the server when it calculates the digest for a managed
- 221 object for which it has access to the key material
- 222 b. The Digest Value
- 223 14. Extensions reported in Query for ExtensionList and ExtensionMap
- 224 15. Application Namespaces reported in Query
- 225 16. Object Types reported in Query other than those noted as required in this profile
- 226 17. Operation Types reported in Query other than those noted as required in this profile (or any
- 227 referenced profile documents)
- 228 18. For TextString attribute values containing test identifiers:
- 229 a. Additional vendor or application prefixes
- 230 19. Additional attributes beyond those noted in the response
- 231

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

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

## 248 **4.7.2 Variable behavior**

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

- 250 1. A test MAY omit the clean-up requests and responses (containing Revoke and/or Destroy) at the
- 251 end of the test provided there is a separate mechanism to remove the created objects during
- 252 testing.
- 253 2. A test MAY omit the test identifiers if the client is unable to include them in requests. This
- 254 includes the following attributes:
- 255 a. Name; and
- 256 b. x-ID
- 257 3. A test MAY perform requests with multiple batch items or as multiple requests with a single batch
- 258 item provided the sequence of operations are equivalent
- 259 4. A request MAY contain an optional *Authentication* [KMIP\_SPEC] structure within each request
- 260

---

## Appendix A. Acknowledgments

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

### Participants:

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

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



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

## Appendix B. KMIP Specification Cross Reference

Reference Term	KMIP 1.0	KMIP 1.1	KMIP 1.2
<b>1 Introduction</b>			
<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.
<b>2 Objects</b>			
<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.
<b>3 Attributes</b>			
<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.

<b>Reference Term</b>	<b>KMIP 1.0</b>	<b>KMIP 1.1</b>	<b>KMIP 1.2</b>
<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.
<b>4 Client-to-Server Operations</b>			
<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.

<b>Reference Term</b>	<b>KMIP 1.0</b>	<b>KMIP 1.1</b>	<b>KMIP 1.2</b>
<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.
<b>5 Server-to-Client Operations</b>			
<i>Notify</i>	5.1.	5.1.	5.1.
<i>Put</i>	5.2.	5.2.	5.2.
<b>6 Message Contents</b>			
<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.
<b>7 Message Format</b>			

<b>Reference Term</b>	<b>KMIP 1.0</b>	<b>KMIP 1.1</b>	<b>KMIP 1.2</b>
<i>Message Structure</i>	7.1.	7.1.	7.1.
<i>Operations</i>	7.2.	7.2.	7.2.
<b>8 Authentication</b>			
<i>Authentication</i>	8	8	8
<b>9 Message Encoding</b>			
<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.

<b>Reference Term</b>	<b>KMIP 1.0</b>	<b>KMIP 1.1</b>	<b>KMIP 1.2</b>
<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.	-	-
<b>10 Transport</b>			
<i>Transport</i>	10	10	10
<b>12 KMIP Server and Client Implementation Conformance</b>			
<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.

371

372

## Appendix C. Revision History

373

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
wd03a	24-October-2013	Tim Hudson	Editorial update to include VendorIdentification in the list of allowed variations as per TC motion.
pr01update	11-June-2014	Tim Hudson	Updated following Public Review

374