KMIP Cryptographic Services Profile Version 1.0

OASIS Standard

19 May 2015

Specification URIs

This version:

http://docs.oasis-open.org/kmip/kmip-cs-profile/v1.0/os/kmip-cs-profile-v1.0-os.doc (Authoritative)
http://docs.oasis-open.org/kmip/kmip-cs-profile/v1.0/os/kmip-cs-profile-v1.0-os.html
http://docs.oasis-open.org/kmip/kmip-cs-profile/v1.0/os/kmip-cs-profile-v1.0-os.pdf

Previous version:

http://docs.oasis-open.org/kmip/kmip-cs-profile/v1.0/csprd01/kmip-cs-profile-v1.0-csprd01.doc (Authoritative)
http://docs.oasis-open.org/kmip/kmip-cs-profile/v1.0/csprd01/kmip-cs-profile-v1.0-csprd01.html
http://docs.oasis-open.org/kmip/kmip-cs-profile/v1.0/csprd01/kmip-cs-profile-v1.0-csprd01.pdf

Latest version:

http://docs.oasis-open.org/kmip/kmip-cs-profile/v1.0/kmip-cs-profile-v1.0.doc (Authoritative)
http://docs.oasis-open.org/kmip/kmip-cs-profile/v1.0/kmip-cs-profile-v1.0.html
http://docs.oasis-open.org/kmip/kmip-cs-profile/v1.0/kmip-cs-profile-v1.0.pdf

Technical Committee:

OASIS Key Management Interoperability Protocol (KMIP) TC

Chairs:

Saikat Saha (saikat.saha@oracle.com), Oracle
Tony Cox (tjc@cryptsoft.com), Cryptsoft Pty Ltd.

Editor:

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

Related work:

This specification is related to:

- *Key Management Interoperability Protocol Profiles Version 1.0.* Edited by Robert Griffin and Subhash Sankuratripati. Latest version: http://docs.oasis-open.org/kmip/profiles/v1.0/kmip-profiles-1.0.html.
- *Key Management Interoperability Protocol Profiles Version 1.1*. Edited by Robert Griffin and Subhash Sankuratripati. Latest version: http://docs.oasis-open.org/kmip/profiles/v1.1/kmip-profiles-v1.1.html.
- *Key Management Interoperability Protocol Profiles Version 1.2*. Edited by Tim Hudson and Robert Lockhart. Latest version: http://docs.oasis-open.org/kmip/profiles/v1.2/kmip-profiles-v1.2.html.
- *Key Management Interoperability Protocol Specification Version 1.1*. Edited by Robert Haas and Indra Fitzgerald. Latest version: http://docs.oasis-open.org/kmip/spec/v1.1/kmip-spec-v1.1.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.

- *Key Management Interoperability Protocol Test Cases Version 1.2*. Edited by Tim Hudson and Faisal Faruqui. Latest version: http://docs.oasis-open.org/kmip/testcases/v1.2/kmip-testcases-v1.2.html.
- *Key Management Interoperability Protocol Usage Guide Version 1.2*. Edited by Indra Fitzgerald and Judith Furlong. Latest version: http://docs.oasis-open.org/kmip/ug/v1.2/kmip-ug-v1.2.html.

Abstract:

Describes the use of KMIP operations to support cryptographic services being performed by a KMIP server on behalf of a KMIP client for key management operations.

Status:

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

Technical Committee members should send comments on this 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-cs-v1.0]

KMIP Cryptographic Services Profile Version 1.0. Edited by Tim Hudson. 19 May 2015. OASIS Standard. http://docs.oasis-open.org/kmip/kmip-cs-profile/v1.0/os/kmip-cs-profile-v1.0-os.html. Latest version: http://docs.oasis-open.org/kmip/kmip-cs-profile/v1.0/kmip-cs-profile-v1.0.html.

Notices

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

For normative definition of the elements of KMIP see the KMIP Specification [KMIP-SPEC-1_2] and the KMIP Profiles [KMIP-PROF-1_2].

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-SPEC-1_2] *Key Management Interoperability Protocol Specification Version 1.2.* Edited by Kiran Thota and Kelley Burgin. Latest version: http://docs.oasis-open.org/kmip/spec/v1.2/kmip-spec-v1.2.doc.

[KMIP-PROF-1_2] *Key Management Interoperability Protocol Profiles Version 1.2*. Edited by Tim Hudson and Robert Lockhart. Latest version: http://docs.oasis-open.org/kmip/profiles/v1.2/kmip-profiles-v1.2.doc.

2 Cryptographic Profiles

The Basic Cryptographic Client and Server profiles specify the use of KMIP to request encryption and decryption operations from a KMIP server.

The Advanced Cryptographic Client and Server profiles specify the use of KMIP to request encryption, decryption, signature, and verification operations from a KMIP server.

The RNG Cryptographic Client and Server profiles specify the use of KMIP to request random number generator operations from a KMIP server.

2.1 Basic Cryptographic Client Profile

A KMIP client conformant to this profile:

1. SHALL conform to the KMIP Baseline Client profile in [KMIP-PROF-1_2] and [KMIP-SPEC-1_2]
2. SHALL support at least one of the *Client-to-Server Operation* [KMIP-SPEC-1_2]:
    a. *Encrypt* [KMIP-SPEC-1_2]
    b. *Decrypt* [KMIP-SPEC-1_2]
3. MAY support any clause within [KMIP-SPEC-1_2] provided it does not conflict with any other clause within this section 2.1
4. MAY support extensions outside the scope of this standard (e.g., vendor extensions, conformance clauses) that do not contradict any KMIP requirements.

2.2 Basic Cryptographic Server Profile

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

1. SHALL conform to the Baseline Server of [KMIP-PROF-1_2]
2. SHALL support the *Client-to-Server Operation* [KMIP-SPEC-1_2]:
    a. *Encrypt* [KMIP-SPEC-1_2]
    b. *Decrypt* [KMIP-SPEC-1_2]
3. MAY support any clause within [KMIP-SPEC-1_2] provided it does not conflict with any other clause within this section 2.2
4. MAY support extensions outside the scope of this standard (e.g., vendor extensions, conformance clauses) that do not contradict any KMIP requirements.

2.3 Advanced Cryptographic Client Profile

A KMIP client conforming to this profile:

1. SHALL conform to the KMIP Baseline Client profile in [KMIP-PROF-1_2] and [KMIP-SPEC-1_2]
2. SHALL support at least one of the *Client-to-Server Operation* [KMIP-SPEC-1_2]:
    a. *Encrypt* [KMIP-SPEC-1_2]
    b. *Decrypt* [KMIP-SPEC-1_2]
    c. *Sign* [KMIP-SPEC-1_2]
    d. *Signature Verify* [KMIP-SPEC-1_2]
    e. *MAC* [KMIP-SPEC-1_2]
    f. *MAC Verify* [KMIP-SPEC-1_2]
    g. *RNG Retrieve* [KMIP-SPEC-1_2]
    h. *RNG Seed* [KMIP-SPEC-1_2]

3. MAY support any clause within [KMIP-SPEC-1_2] provided it does not conflict with any other clause within this section 2.3
4. MAY support extensions outside the scope of this standard (e.g., vendor extensions, conformance clauses) that do not contradict any KMIP requirements.

2.4 Advanced Cryptographic Server Profile

A KMIP server conforming to this profile:

1. SHALL conform to the KMIP Baseline Server profile in [KMIP-PROF-1_2] and [KMIP-SPEC-1_2]
2. SHALL support the *Client-to-Server Operation* [KMIP-SPEC-1_2]:
    a. *Encrypt* [KMIP-SPEC-1_2]
    b. *Decrypt* [KMIP-SPEC-1_2]
    c. *Sign* [KMIP-SPEC-1_2]
    d. *Signature Verify* [KMIP-SPEC-1_2]
    e. *MAC* [KMIP-SPEC-1_2]
    f. *MAC Verify* [KMIP-SPEC-1_2]
    g. *RNG Retrieve* [KMIP-SPEC-1_2]
    h. *RNG Seed* [KMIP-SPEC-1_2]
3. MAY support any clause within [KMIP-SPEC-1_2] provided it does not conflict with any other clause within this section 2.4
4. MAY support extensions outside the scope of this standard (e.g., vendor extensions, conformance clauses) that do not contradict any KMIP requirements.

2.5 RNG Cryptographic Client Profile

A KMIP client conformant to this profile:

1. SHALL conform to the KMIP Baseline Client profile in [KMIP-PROF-1_2] and [KMIP-SPEC-1_2]
2. SHALL support at least one of the *Client-to-Server Operation* [KMIP-SPEC-1_2]:
    a. *RNG Retrieve* [KMIP-SPEC-1_2]
    b. *RNG Seed* [KMIP-SPEC-1_2]
3. MAY support any clause within [KMIP-SPEC-1_2] provided it does not conflict with any other clause within this section 2.5
4. MAY support extensions outside the scope of this standard (e.g., vendor extensions, conformance clauses) that do not contradict any KMIP requirements.

2.6 RNG Cryptographic Server Profile

A KMIP server conforming to this profile:

1. SHALL conform to the KMIP Baseline Server profile in [KMIP-PROF-1_2] and [KMIP-SPEC-1_2]
2. SHALL support the *Client-to-Server Operation* [KMIP-SPEC-1_2]:
    a. *RNG Retrieve* [KMIP-SPEC-1_2]
    b. *RNG Seed* [KMIP-SPEC-1_2]
3. MAY support any clause within [KMIP-SPEC-1_2] provided it does not conflict with any other clause within this section 2.6
4. MAY support extensions outside the scope of this standard (e.g., vendor extensions, conformance clauses) that do not contradict any KMIP requirements.

3 Cryptographic Profile Test Cases

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

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

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

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

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

3.1 Mandatory Test Cases KMIP v1.2 - Basic

3.1.1 CS-BC-M-1-12 - Encrypt with New Symmetric Key

Create a symmetric key and perform encrypt using the symmetric key.

```
      # TIME 0
0001  <RequestMessage>
0002    <RequestHeader>
0003      <ProtocolVersion>
0004        <ProtocolVersionMajor type="Integer" value="1"/>
0005        <ProtocolVersionMinor type="Integer" value="2"/>
0006      </ProtocolVersion>
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="Create"/>
0011      <RequestPayload>
0012        <ObjectType type="Enumeration" value="SymmetricKey"/>
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
      Algorithm"/>
0016            <AttributeValue type="Enumeration" value="AES"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="Cryptographic
      Length"/>
0020            <AttributeValue type="Integer" value="128"/>
0021          </Attribute>
0022          <Attribute>
0023            <AttributeName type="TextString" value="Cryptographic
      Usage Mask"/>
0024            <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025          </Attribute>
0026          <Attribute>
0027            <AttributeName type="TextString" value="Name"/>
0028            <AttributeValue>
```

```
0029              <NameValue type="TextString" value="CS-BC-M-1-12"/>
0030              <NameType type="Enumeration"
      value="UninterpretedTextString"/>
0031            </AttributeValue>
0032          </Attribute>
0033          <Attribute>
0034            <AttributeName type="TextString" value="Cryptographic
      Parameters"/>
0035            <AttributeValue>
0036              <BlockCipherMode type="Enumeration" value="ECB"/>
0037            </AttributeValue>
0038          </Attribute>
0039          <Attribute>
0040            <AttributeName type="TextString" value="Activation Date"/>
0041            <AttributeValue type="DateTime" value="$NOW-3600"/>
0042          </Attribute>
0043        </TemplateAttribute>
0044      </RequestPayload>
0045    </BatchItem>
0046  </RequestMessage>
```

```
0047  <ResponseMessage>
0048    <ResponseHeader>
0049      <ProtocolVersion>
0050        <ProtocolVersionMajor type="Integer" value="1"/>
0051        <ProtocolVersionMinor type="Integer" value="2"/>
0052      </ProtocolVersion>
0053      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0054      <BatchCount type="Integer" value="1"/>
0055    </ResponseHeader>
0056    <BatchItem>
0057      <Operation type="Enumeration" value="Create"/>
0058      <ResultStatus type="Enumeration" value="Success"/>
0059      <ResponsePayload>
0060        <ObjectType type="Enumeration" value="SymmetricKey"/>
0061        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0062      </ResponsePayload>
0063    </BatchItem>
0064  </ResponseMessage>
```

```
      # TIME 1
0065  <RequestMessage>
0066    <RequestHeader>
0067      <ProtocolVersion>
0068        <ProtocolVersionMajor type="Integer" value="1"/>
0069        <ProtocolVersionMinor type="Integer" value="2"/>
0070      </ProtocolVersion>
0071      <BatchCount type="Integer" value="1"/>
0072    </RequestHeader>
0073    <BatchItem>
0074      <Operation type="Enumeration" value="Encrypt"/>
0075      <RequestPayload>
0076        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0077        <Data type="ByteString"
      value="0102030405060708091011121314151 6"/>
0078      </RequestPayload>
0079    </BatchItem>
0080  </RequestMessage>
```

```
0081 <ResponseMessage>
0082   <ResponseHeader>
0083     <ProtocolVersion>
0084       <ProtocolVersionMajor type="Integer" value="1"/>
0085       <ProtocolVersionMinor type="Integer" value="2"/>
0086     </ProtocolVersion>
0087     <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0088     <BatchCount type="Integer" value="1"/>
0089   </ResponseHeader>
0090   <BatchItem>
0091     <Operation type="Enumeration" value="Encrypt"/>
0092     <ResultStatus type="Enumeration" value="Success"/>
0093     <ResponsePayload>
0094       <UniqueIdentifier type="TextString"
       value="$UNIQUE_IDENTIFIER_0"/>
0095       <Data type="ByteString"
       value="fd912d102dbb482f6f6e91bd57119095"/>
0096     </ResponsePayload>
0097   </BatchItem>
0098 </ResponseMessage>
```

```
       # TIME 2
0099 <RequestMessage>
0100   <RequestHeader>
0101     <ProtocolVersion>
0102       <ProtocolVersionMajor type="Integer" value="1"/>
0103       <ProtocolVersionMinor type="Integer" value="2"/>
0104     </ProtocolVersion>
0105     <BatchCount type="Integer" value="1"/>
0106   </RequestHeader>
0107   <BatchItem>
0108     <Operation type="Enumeration" value="Revoke"/>
0109     <RequestPayload>
0110       <UniqueIdentifier type="TextString"
       value="$UNIQUE_IDENTIFIER_0"/>
0111       <RevocationReason>
0112         <RevocationReasonCode type="Enumeration"
       value="Unspecified"/>
0113       </RevocationReason>
0114     </RequestPayload>
0115   </BatchItem>
0116 </RequestMessage>
```

```
0117 <ResponseMessage>
0118   <ResponseHeader>
0119     <ProtocolVersion>
0120       <ProtocolVersionMajor type="Integer" value="1"/>
0121       <ProtocolVersionMinor type="Integer" value="2"/>
0122     </ProtocolVersion>
0123     <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0124     <BatchCount type="Integer" value="1"/>
0125   </ResponseHeader>
0126   <BatchItem>
0127     <Operation type="Enumeration" value="Revoke"/>
0128     <ResultStatus type="Enumeration" value="Success"/>
0129     <ResponsePayload>
0130       <UniqueIdentifier type="TextString"
       value="$UNIQUE_IDENTIFIER_0"/>
0131     </ResponsePayload>
0132   </BatchItem>
```

```
0133 </ResponseMessage>
     # TIME 3
0134 <RequestMessage>
0135   <RequestHeader>
0136     <ProtocolVersion>
0137       <ProtocolVersionMajor type="Integer" value="1"/>
0138       <ProtocolVersionMinor type="Integer" value="2"/>
0139     </ProtocolVersion>
0140     <BatchCount type="Integer" value="1"/>
0141   </RequestHeader>
0142   <BatchItem>
0143     <Operation type="Enumeration" value="Destroy"/>
0144     <RequestPayload>
0145       <UniqueIdentifier type="TextString"
     value="$UNIQUE_IDENTIFIER_0"/>
0146     </RequestPayload>
0147   </BatchItem>
0148 </RequestMessage>
0149 <ResponseMessage>
0150   <ResponseHeader>
0151     <ProtocolVersion>
0152       <ProtocolVersionMajor type="Integer" value="1"/>
0153       <ProtocolVersionMinor type="Integer" value="2"/>
0154     </ProtocolVersion>
0155     <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0156     <BatchCount type="Integer" value="1"/>
0157   </ResponseHeader>
0158   <BatchItem>
0159     <Operation type="Enumeration" value="Destroy"/>
0160     <ResultStatus type="Enumeration" value="Success"/>
0161     <ResponsePayload>
0162       <UniqueIdentifier type="TextString"
     value="$UNIQUE_IDENTIFIER_0"/>
0163     </ResponsePayload>
0164   </BatchItem>
0165 </ResponseMessage>
```

115

116 3.1.2 CS-BC-M-2-12 - Decrypt with New Symmetric Key

117 Create a symmetric key and perform decrypt using the symmetric key. Note: Create followed by Decrypt
118 is unusual but some applications actually do this relying on Decrypt and Encrypt being able to be used
119 around the 'wrong' way to get the same result.

120

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

```
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
      Algorithm"/>
0016            <AttributeValue type="Enumeration" value="AES"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="Cryptographic
      Length"/>
0020            <AttributeValue type="Integer" value="128"/>
0021          </Attribute>
0022          <Attribute>
0023            <AttributeName type="TextString" value="Cryptographic
      Usage Mask"/>
0024            <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025          </Attribute>
0026          <Attribute>
0027            <AttributeName type="TextString" value="Name"/>
0028            <AttributeValue>
0029              <NameValue type="TextString" value="CS-BC-M-2-12"/>
0030              <NameType type="Enumeration"
      value="UninterpretedTextString"/>
0031            </AttributeValue>
0032          </Attribute>
0033          <Attribute>
0034            <AttributeName type="TextString" value="Cryptographic
      Parameters"/>
0035            <AttributeValue>
0036              <BlockCipherMode type="Enumeration" value="ECB"/>
0037            </AttributeValue>
0038          </Attribute>
0039          <Attribute>
0040            <AttributeName type="TextString" value="Activation Date"/>
0041            <AttributeValue type="DateTime" value="$NOW-3600"/>
0042          </Attribute>
0043        </TemplateAttribute>
0044      </RequestPayload>
0045    </BatchItem>
0046  </RequestMessage>
```

```
0047  <ResponseMessage>
0048    <ResponseHeader>
0049      <ProtocolVersion>
0050        <ProtocolVersionMajor type="Integer" value="1"/>
0051        <ProtocolVersionMinor type="Integer" value="2"/>
0052      </ProtocolVersion>
0053      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0054      <BatchCount type="Integer" value="1"/>
0055    </ResponseHeader>
0056    <BatchItem>
0057      <Operation type="Enumeration" value="Create"/>
0058      <ResultStatus type="Enumeration" value="Success"/>
0059      <ResponsePayload>
0060        <ObjectType type="Enumeration" value="SymmetricKey"/>
0061        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0062      </ResponsePayload>
0063    </BatchItem>
0064  </ResponseMessage>
```

```
      # TIME 1
0065  <RequestMessage>
0066    <RequestHeader>
0067      <ProtocolVersion>
0068        <ProtocolVersionMajor type="Integer" value="1"/>
0069        <ProtocolVersionMinor type="Integer" value="2"/>
0070      </ProtocolVersion>
0071      <BatchCount type="Integer" value="1"/>
0072    </RequestHeader>
0073    <BatchItem>
0074      <Operation type="Enumeration" value="Decrypt"/>
0075      <RequestPayload>
0076        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0077        <Data type="ByteString"
      value="fd912d102dbb482f6f6e91bd57119095"/>
0078      </RequestPayload>
0079    </BatchItem>
0080  </RequestMessage>
```

```
0081  <ResponseMessage>
0082    <ResponseHeader>
0083      <ProtocolVersion>
0084        <ProtocolVersionMajor type="Integer" value="1"/>
0085        <ProtocolVersionMinor type="Integer" value="2"/>
0086      </ProtocolVersion>
0087      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0088      <BatchCount type="Integer" value="1"/>
0089    </ResponseHeader>
0090    <BatchItem>
0091      <Operation type="Enumeration" value="Decrypt"/>
0092      <ResultStatus type="Enumeration" value="Success"/>
0093      <ResponsePayload>
0094        <UniqueIdentifier type="TextString"
      value="$UNIQUE IDENTIFIER 0"/>
0095        <Data type="ByteString"
      value="0102030405060708091011121314151 6"/>
0096      </ResponsePayload>
0097    </BatchItem>
0098  </ResponseMessage>
```

```
      # TIME 2
0099  <RequestMessage>
0100    <RequestHeader>
0101      <ProtocolVersion>
0102        <ProtocolVersionMajor type="Integer" value="1"/>
0103        <ProtocolVersionMinor type="Integer" value="2"/>
0104      </ProtocolVersion>
0105      <BatchCount type="Integer" value="1"/>
0106    </RequestHeader>
0107    <BatchItem>
0108      <Operation type="Enumeration" value="Revoke"/>
0109      <RequestPayload>
0110        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0111        <RevocationReason>
0112          <RevocationReasonCode type="Enumeration"
      value="Unspecified"/>
0113        </RevocationReason>
0114      </RequestPayload>
```

```
0115    </BatchItem>
0116  </RequestMessage>
```

```
0117  <ResponseMessage>
0118    <ResponseHeader>
0119      <ProtocolVersion>
0120        <ProtocolVersionMajor type="Integer" value="1"/>
0121        <ProtocolVersionMinor type="Integer" value="2"/>
0122      </ProtocolVersion>
0123      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0124      <BatchCount type="Integer" value="1"/>
0125    </ResponseHeader>
0126    <BatchItem>
0127      <Operation type="Enumeration" value="Revoke"/>
0128      <ResultStatus type="Enumeration" value="Success"/>
0129      <ResponsePayload>
0130        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0131      </ResponsePayload>
0132    </BatchItem>
0133  </ResponseMessage>
```

```
      # TIME 3
0134  <RequestMessage>
0135    <RequestHeader>
0136      <ProtocolVersion>
0137        <ProtocolVersionMajor type="Integer" value="1"/>
0138        <ProtocolVersionMinor type="Integer" value="2"/>
0139      </ProtocolVersion>
0140      <BatchCount type="Integer" value="1"/>
0141    </RequestHeader>
0142    <BatchItem>
0143      <Operation type="Enumeration" value="Destroy"/>
0144      <RequestPayload>
0145        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0146      </RequestPayload>
0147    </BatchItem>
0148  </RequestMessage>
```

```
0149  <ResponseMessage>
0150    <ResponseHeader>
0151      <ProtocolVersion>
0152        <ProtocolVersionMajor type="Integer" value="1"/>
0153        <ProtocolVersionMinor type="Integer" value="2"/>
0154      </ProtocolVersion>
0155      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0156      <BatchCount type="Integer" value="1"/>
0157    </ResponseHeader>
0158    <BatchItem>
0159      <Operation type="Enumeration" value="Destroy"/>
0160      <ResultStatus type="Enumeration" value="Success"/>
0161      <ResponsePayload>
0162        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0163      </ResponsePayload>
0164    </BatchItem>
0165  </ResponseMessage>
```

121

3.1.3 CS-BC-M-3-12 - Encrypt and Decrypt with New Symmetric Key

Create a symmetric key and perform both encrypt and decrypt operations using the symmetric key.

```
      # TIME 0
0001  <RequestMessage>
0002    <RequestHeader>
0003      <ProtocolVersion>
0004        <ProtocolVersionMajor type="Integer" value="1"/>
0005        <ProtocolVersionMinor type="Integer" value="2"/>
0006      </ProtocolVersion>
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="Create"/>
0011      <RequestPayload>
0012        <ObjectType type="Enumeration" value="SymmetricKey"/>
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
      Algorithm"/>
0016            <AttributeValue type="Enumeration" value="AES"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="Cryptographic
      Length"/>
0020            <AttributeValue type="Integer" value="128"/>
0021          </Attribute>
0022          <Attribute>
0023            <AttributeName type="TextString" value="Cryptographic
      Usage Mask"/>
0024            <AttributeValue type="Integer" value="Decrypt Encrypt"/>
0025          </Attribute>
0026          <Attribute>
0027            <AttributeName type="TextString" value="Name"/>
0028            <AttributeValue>
0029              <NameValue type="TextString" value="CS-BC-M-3-12"/>
0030              <NameType type="Enumeration"
      value="UninterpretedTextString"/>
0031            </AttributeValue>
0032          </Attribute>
0033          <Attribute>
0034            <AttributeName type="TextString" value="Cryptographic
      Parameters"/>
0035            <AttributeValue>
0036              <BlockCipherMode type="Enumeration" value="ECB"/>
0037            </AttributeValue>
0038          </Attribute>
0039          <Attribute>
0040            <AttributeName type="TextString" value="Activation Date"/>
0041            <AttributeValue type="DateTime" value="$NOW-3600"/>
0042          </Attribute>
0043        </TemplateAttribute>
0044      </RequestPayload>
0045    </BatchItem>
0046  </RequestMessage>
0047  <ResponseMessage>
0048    <ResponseHeader>
0049      <ProtocolVersion>
```

```
0050        <ProtocolVersionMajor type="Integer" value="1"/>
0051        <ProtocolVersionMinor type="Integer" value="2"/>
0052      </ProtocolVersion>
0053      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0054      <BatchCount type="Integer" value="1"/>
0055    </ResponseHeader>
0056    <BatchItem>
0057      <Operation type="Enumeration" value="Create"/>
0058      <ResultStatus type="Enumeration" value="Success"/>
0059      <ResponsePayload>
0060        <ObjectType type="Enumeration" value="SymmetricKey"/>
0061        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0062      </ResponsePayload>
0063    </BatchItem>
0064  </ResponseMessage>
```

```
      # TIME 1
0065  <RequestMessage>
0066    <RequestHeader>
0067      <ProtocolVersion>
0068        <ProtocolVersionMajor type="Integer" value="1"/>
0069        <ProtocolVersionMinor type="Integer" value="2"/>
0070      </ProtocolVersion>
0071      <BatchCount type="Integer" value="1"/>
0072    </RequestHeader>
0073    <BatchItem>
0074      <Operation type="Enumeration" value="Encrypt"/>
0075      <RequestPayload>
0076        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0077        <Data type="ByteString"
      value="0102030405060708091011121314151 6"/>
0078      </RequestPayload>
0079    </BatchItem>
0080  </RequestMessage>
```

```
0081  <ResponseMessage>
0082    <ResponseHeader>
0083      <ProtocolVersion>
0084        <ProtocolVersionMajor type="Integer" value="1"/>
0085        <ProtocolVersionMinor type="Integer" value="2"/>
0086      </ProtocolVersion>
0087      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0088      <BatchCount type="Integer" value="1"/>
0089    </ResponseHeader>
0090    <BatchItem>
0091      <Operation type="Enumeration" value="Encrypt"/>
0092      <ResultStatus type="Enumeration" value="Success"/>
0093      <ResponsePayload>
0094        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0095        <Data type="ByteString"
      value="fd912d102dbb482f6f6e91bd57119095"/>
0096      </ResponsePayload>
0097    </BatchItem>
0098  </ResponseMessage>
```

```
      # TIME 2
0099  <RequestMessage>
0100    <RequestHeader>
```

```
0101        <ProtocolVersion>
0102          <ProtocolVersionMajor type="Integer" value="1"/>
0103          <ProtocolVersionMinor type="Integer" value="2"/>
0104        </ProtocolVersion>
0105        <BatchCount type="Integer" value="1"/>
0106      </RequestHeader>
0107      <BatchItem>
0108        <Operation type="Enumeration" value="Decrypt"/>
0109        <RequestPayload>
0110          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0111          <Data type="ByteString"
          value="fd912d102dbb482f6f6e91bd57119095"/>
0112        </RequestPayload>
0113      </BatchItem>
0114    </RequestMessage>
0115    <ResponseMessage>
0116      <ResponseHeader>
0117        <ProtocolVersion>
0118          <ProtocolVersionMajor type="Integer" value="1"/>
0119          <ProtocolVersionMinor type="Integer" value="2"/>
0120        </ProtocolVersion>
0121        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0122        <BatchCount type="Integer" value="1"/>
0123      </ResponseHeader>
0124      <BatchItem>
0125        <Operation type="Enumeration" value="Decrypt"/>
0126        <ResultStatus type="Enumeration" value="Success"/>
0127        <ResponsePayload>
0128          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0129          <Data type="ByteString"
          value="0102030405060708091011121314151 6"/>
0130        </ResponsePayload>
0131      </BatchItem>
0132    </ResponseMessage>
          # TIME 3
0133    <RequestMessage>
0134      <RequestHeader>
0135        <ProtocolVersion>
0136          <ProtocolVersionMajor type="Integer" value="1"/>
0137          <ProtocolVersionMinor type="Integer" value="2"/>
0138        </ProtocolVersion>
0139        <BatchCount type="Integer" value="1"/>
0140      </RequestHeader>
0141      <BatchItem>
0142        <Operation type="Enumeration" value="Revoke"/>
0143        <RequestPayload>
0144          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0145          <RevocationReason>
0146            <RevocationReasonCode type="Enumeration"
          value="Unspecified"/>
0147          </RevocationReason>
0148        </RequestPayload>
0149      </BatchItem>
0150    </RequestMessage>
0151    <ResponseMessage>
```

```
0152    <ResponseHeader>
0153      <ProtocolVersion>
0154        <ProtocolVersionMajor type="Integer" value="1"/>
0155        <ProtocolVersionMinor type="Integer" value="2"/>
0156      </ProtocolVersion>
0157      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0158      <BatchCount type="Integer" value="1"/>
0159    </ResponseHeader>
0160    <BatchItem>
0161      <Operation type="Enumeration" value="Revoke"/>
0162      <ResultStatus type="Enumeration" value="Success"/>
0163      <ResponsePayload>
0164        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0165      </ResponsePayload>
0166    </BatchItem>
0167  </ResponseMessage>
```

```
        # TIME 4
0168  <RequestMessage>
0169    <RequestHeader>
0170      <ProtocolVersion>
0171        <ProtocolVersionMajor type="Integer" value="1"/>
0172        <ProtocolVersionMinor type="Integer" value="2"/>
0173      </ProtocolVersion>
0174      <BatchCount type="Integer" value="1"/>
0175    </RequestHeader>
0176    <BatchItem>
0177      <Operation type="Enumeration" value="Destroy"/>
0178      <RequestPayload>
0179        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0180      </RequestPayload>
0181    </BatchItem>
0182  </RequestMessage>
```

```
0183  <ResponseMessage>
0184    <ResponseHeader>
0185      <ProtocolVersion>
0186        <ProtocolVersionMajor type="Integer" value="1"/>
0187        <ProtocolVersionMinor type="Integer" value="2"/>
0188      </ProtocolVersion>
0189      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0190      <BatchCount type="Integer" value="1"/>
0191    </ResponseHeader>
0192    <BatchItem>
0193      <Operation type="Enumeration" value="Destroy"/>
0194      <ResultStatus type="Enumeration" value="Success"/>
0195      <ResponsePayload>
0196        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0197      </ResponsePayload>
0198    </BatchItem>
0199  </ResponseMessage>
```

124

125 3.1.4 CS-BC-M-4-12 - Encrypt with Known Symmetric Key

126 Register a symmetric key and perform encrypt using the symmetric key.

```
        # TIME 0
0001    <RequestMessage>
0002      <RequestHeader>
0003        <ProtocolVersion>
0004          <ProtocolVersionMajor type="Integer" value="1"/>
0005          <ProtocolVersionMinor type="Integer" value="2"/>
0006        </ProtocolVersion>
0007        <BatchCount type="Integer" value="1"/>
0008      </RequestHeader>
0009      <BatchItem>
0010        <Operation type="Enumeration" value="Register"/>
0011        <RequestPayload>
0012          <ObjectType type="Enumeration" value="SymmetricKey"/>
0013          <TemplateAttribute>
0014            <Attribute>
0015              <AttributeName type="TextString" value="Cryptographic
        Usage Mask"/>
0016              <AttributeValue type="Integer" value="Encrypt Decrypt"/>
0017            </Attribute>
0018            <Attribute>
0019              <AttributeName type="TextString" value="x-ID"/>
0020              <AttributeValue type="TextString" value="CS-BC-M-4-12"/>
0021            </Attribute>
0022            <Attribute>
0023              <AttributeName type="TextString" value="Activation Date"/>
0024              <AttributeValue type="DateTime" value="$NOW-3600"/>
0025            </Attribute>
0026          </TemplateAttribute>
0027          <SymmetricKey>
0028            <KeyBlock>
0029              <KeyFormatType type="Enumeration" value="Raw"/>
0030              <KeyValue>
0031                <KeyMaterial type="ByteString"
        value="0123456789abcdef0123456789abcdef"/>
0032              </KeyValue>
0033              <CryptographicAlgorithm type="Enumeration" value="AES"/>
0034              <CryptographicLength type="Integer" value="128"/>
0035            </KeyBlock>
0036          </SymmetricKey>
0037        </RequestPayload>
0038      </BatchItem>
0039    </RequestMessage>
```

```
0040    <ResponseMessage>
0041      <ResponseHeader>
0042        <ProtocolVersion>
0043          <ProtocolVersionMajor type="Integer" value="1"/>
0044          <ProtocolVersionMinor type="Integer" value="2"/>
0045        </ProtocolVersion>
0046        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0047        <BatchCount type="Integer" value="1"/>
0048      </ResponseHeader>
0049      <BatchItem>
0050        <Operation type="Enumeration" value="Register"/>
0051        <ResultStatus type="Enumeration" value="Success"/>
0052        <ResponsePayload>
0053          <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0054        </ResponsePayload>
```

```
0055      </BatchItem>
0056    </ResponseMessage>
```

```
          # TIME 1
0057    <RequestMessage>
0058      <RequestHeader>
0059        <ProtocolVersion>
0060          <ProtocolVersionMajor type="Integer" value="1"/>
0061          <ProtocolVersionMinor type="Integer" value="2"/>
0062        </ProtocolVersion>
0063        <BatchCount type="Integer" value="1"/>
0064      </RequestHeader>
0065      <BatchItem>
0066        <Operation type="Enumeration" value="Encrypt"/>
0067        <RequestPayload>
0068          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0069          <CryptographicParameters>
0070          <BlockCipherMode type="Enumeration" value="ECB"/>
0071          </CryptographicParameters>
0072          <Data type="ByteString"
          value="0102030405060708091011121314151 6"/>
0073        </RequestPayload>
0074      </BatchItem>
0075    </RequestMessage>
```

```
0076    <ResponseMessage>
0077      <ResponseHeader>
0078        <ProtocolVersion>
0079          <ProtocolVersionMajor type="Integer" value="1"/>
0080          <ProtocolVersionMinor type="Integer" value="2"/>
0081        </ProtocolVersion>
0082        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0083        <BatchCount type="Integer" value="1"/>
0084      </ResponseHeader>
0085      <BatchItem>
0086        <Operation type="Enumeration" value="Encrypt"/>
0087        <ResultStatus type="Enumeration" value="Success"/>
0088        <ResponsePayload>
0089          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0090          <Data type="ByteString"
          value="d9bcce11b0b437b90239552df3a360c9"/>
0091        </ResponsePayload>
0092      </BatchItem>
0093    </ResponseMessage>
```

```
          # TIME 2
0094    <RequestMessage>
0095      <RequestHeader>
0096        <ProtocolVersion>
0097          <ProtocolVersionMajor type="Integer" value="1"/>
0098          <ProtocolVersionMinor type="Integer" value="2"/>
0099        </ProtocolVersion>
0100        <BatchCount type="Integer" value="1"/>
0101      </RequestHeader>
0102      <BatchItem>
0103        <Operation type="Enumeration" value="Revoke"/>
0104        <RequestPayload>
0105          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
```

```
0106        <RevocationReason>
0107          <RevocationReasonCode type="Enumeration"
      value="Unspecified"/>
0108        </RevocationReason>
0109      </RequestPayload>
0110    </BatchItem>
0111  </RequestMessage>
```

```
0112  <ResponseMessage>
0113    <ResponseHeader>
0114      <ProtocolVersion>
0115        <ProtocolVersionMajor type="Integer" value="1"/>
0116        <ProtocolVersionMinor type="Integer" value="2"/>
0117      </ProtocolVersion>
0118      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0119      <BatchCount type="Integer" value="1"/>
0120    </ResponseHeader>
0121    <BatchItem>
0122      <Operation type="Enumeration" value="Revoke"/>
0123      <ResultStatus type="Enumeration" value="Success"/>
0124      <ResponsePayload>
0125        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0126      </ResponsePayload>
0127    </BatchItem>
0128  </ResponseMessage>
```

```
      # TIME 3
0129  <RequestMessage>
0130    <RequestHeader>
0131      <ProtocolVersion>
0132        <ProtocolVersionMajor type="Integer" value="1"/>
0133        <ProtocolVersionMinor type="Integer" value="2"/>
0134      </ProtocolVersion>
0135      <BatchCount type="Integer" value="1"/>
0136    </RequestHeader>
0137    <BatchItem>
0138      <Operation type="Enumeration" value="Destroy"/>
0139      <RequestPayload>
0140        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0141      </RequestPayload>
0142    </BatchItem>
0143  </RequestMessage>
```

```
0144  <ResponseMessage>
0145    <ResponseHeader>
0146      <ProtocolVersion>
0147        <ProtocolVersionMajor type="Integer" value="1"/>
0148        <ProtocolVersionMinor type="Integer" value="2"/>
0149      </ProtocolVersion>
0150      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0151      <BatchCount type="Integer" value="1"/>
0152    </ResponseHeader>
0153    <BatchItem>
0154      <Operation type="Enumeration" value="Destroy"/>
0155      <ResultStatus type="Enumeration" value="Success"/>
0156      <ResponsePayload>
0157        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0158      </ResponsePayload>
```

```
0159    </BatchItem>
0160  </ResponseMessage>
```

127

128 3.1.5 CS-BC-M-5-12 - Decrypt with Known Symmetric Key

129 Register a symmetric key and perform decrypt using the symmetric key. Note: Register followed by
130 Decrypt is unusual but some applications actually do this relying on Decrypt and Encrypt being able to be
131 used around the 'wrong' way to get the same result.

132

```
      # TIME 0
0001  <RequestMessage>
0002    <RequestHeader>
0003      <ProtocolVersion>
0004        <ProtocolVersionMajor type="Integer" value="1"/>
0005        <ProtocolVersionMinor type="Integer" value="2"/>
0006      </ProtocolVersion>
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="Register"/>
0011      <RequestPayload>
0012        <ObjectType type="Enumeration" value="SymmetricKey"/>
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
      Usage Mask"/>
0016            <AttributeValue type="Integer" value="Encrypt Decrypt"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="x-ID"/>
0020            <AttributeValue type="TextString" value="CS-BC-M-5-12"/>
0021          </Attribute>
0022          <Attribute>
0023            <AttributeName type="TextString" value="Activation Date"/>
0024            <AttributeValue type="DateTime" value="$NOW-3600"/>
0025          </Attribute>
0026        </TemplateAttribute>
0027        <SymmetricKey>
0028          <KeyBlock>
0029            <KeyFormatType type="Enumeration" value="Raw"/>
0030            <KeyValue>
0031              <KeyMaterial type="ByteString"
      value="0123456789abcdef0123456789abcdef"/>
0032            </KeyValue>
0033            <CryptographicAlgorithm type="Enumeration" value="AES"/>
0034            <CryptographicLength type="Integer" value="128"/>
0035          </KeyBlock>
0036        </SymmetricKey>
0037      </RequestPayload>
0038    </BatchItem>
0039  </RequestMessage>
```

```
0040  <ResponseMessage>
0041    <ResponseHeader>
0042      <ProtocolVersion>
0043        <ProtocolVersionMajor type="Integer" value="1"/>
0044        <ProtocolVersionMinor type="Integer" value="2"/>
```

```
0045      </ProtocolVersion>
0046      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0047      <BatchCount type="Integer" value="1"/>
0048    </ResponseHeader>
0049    <BatchItem>
0050      <Operation type="Enumeration" value="Register"/>
0051      <ResultStatus type="Enumeration" value="Success"/>
0052      <ResponsePayload>
0053        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0054      </ResponsePayload>
0055    </BatchItem>
0056  </ResponseMessage>
```

```
        # TIME 1
0057  <RequestMessage>
0058    <RequestHeader>
0059      <ProtocolVersion>
0060        <ProtocolVersionMajor type="Integer" value="1"/>
0061        <ProtocolVersionMinor type="Integer" value="2"/>
0062      </ProtocolVersion>
0063      <BatchCount type="Integer" value="1"/>
0064    </RequestHeader>
0065    <BatchItem>
0066      <Operation type="Enumeration" value="Decrypt"/>
0067      <RequestPayload>
0068        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0069        <CryptographicParameters>
0070        <BlockCipherMode type="Enumeration" value="ECB"/>
0071        </CryptographicParameters>
0072        <Data type="ByteString"
      value="d9bcce11b0b437b90239552df3a360c9"/>
0073      </RequestPayload>
0074    </BatchItem>
0075  </RequestMessage>
```

```
0076  <ResponseMessage>
0077    <ResponseHeader>
0078      <ProtocolVersion>
0079        <ProtocolVersionMajor type="Integer" value="1"/>
0080        <ProtocolVersionMinor type="Integer" value="2"/>
0081      </ProtocolVersion>
0082      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0083      <BatchCount type="Integer" value="1"/>
0084    </ResponseHeader>
0085    <BatchItem>
0086      <Operation type="Enumeration" value="Decrypt"/>
0087      <ResultStatus type="Enumeration" value="Success"/>
0088      <ResponsePayload>
0089        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0090        <Data type="ByteString"
      value="0102030405060708091011121314151 6"/>
0091      </ResponsePayload>
0092    </BatchItem>
0093  </ResponseMessage>
```

```
        # TIME 2
0094  <RequestMessage>
0095    <RequestHeader>
```

```
0096      <ProtocolVersion>
0097        <ProtocolVersionMajor type="Integer" value="1"/>
0098        <ProtocolVersionMinor type="Integer" value="2"/>
0099      </ProtocolVersion>
0100      <BatchCount type="Integer" value="1"/>
0101    </RequestHeader>
0102    <BatchItem>
0103      <Operation type="Enumeration" value="Revoke"/>
0104      <RequestPayload>
0105        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0106        <RevocationReason>
0107          <RevocationReasonCode type="Enumeration"
        value="Unspecified"/>
0108        </RevocationReason>
0109      </RequestPayload>
0110    </BatchItem>
0111  </RequestMessage>
```

```
0112  <ResponseMessage>
0113    <ResponseHeader>
0114      <ProtocolVersion>
0115        <ProtocolVersionMajor type="Integer" value="1"/>
0116        <ProtocolVersionMinor type="Integer" value="2"/>
0117      </ProtocolVersion>
0118      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0119      <BatchCount type="Integer" value="1"/>
0120    </ResponseHeader>
0121    <BatchItem>
0122      <Operation type="Enumeration" value="Revoke"/>
0123      <ResultStatus type="Enumeration" value="Success"/>
0124      <ResponsePayload>
0125        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0126      </ResponsePayload>
0127    </BatchItem>
0128  </ResponseMessage>
```

```
        # TIME 3
0129  <RequestMessage>
0130    <RequestHeader>
0131      <ProtocolVersion>
0132        <ProtocolVersionMajor type="Integer" value="1"/>
0133        <ProtocolVersionMinor type="Integer" value="2"/>
0134      </ProtocolVersion>
0135      <BatchCount type="Integer" value="1"/>
0136    </RequestHeader>
0137    <BatchItem>
0138      <Operation type="Enumeration" value="Destroy"/>
0139      <RequestPayload>
0140        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0141      </RequestPayload>
0142    </BatchItem>
0143  </RequestMessage>
```

```
0144  <ResponseMessage>
0145    <ResponseHeader>
0146      <ProtocolVersion>
0147        <ProtocolVersionMajor type="Integer" value="1"/>
0148        <ProtocolVersionMinor type="Integer" value="2"/>
```

```
0149      </ProtocolVersion>
0150      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0151      <BatchCount type="Integer" value="1"/>
0152    </ResponseHeader>
0153    <BatchItem>
0154      <Operation type="Enumeration" value="Destroy"/>
0155      <ResultStatus type="Enumeration" value="Success"/>
0156      <ResponsePayload>
0157        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0158      </ResponsePayload>
0159    </BatchItem>
0160  </ResponseMessage>
```

133

134 3.1.6 CS-BC-M-6-12 - Encrypt and Decrypt with Known Symmetric Key

135 Register a symmetric key and perform both encrypt and decrypt operations using the symmetric key.

```
        # TIME 0
0001    <RequestMessage>
0002      <RequestHeader>
0003        <ProtocolVersion>
0004          <ProtocolVersionMajor type="Integer" value="1"/>
0005          <ProtocolVersionMinor type="Integer" value="2"/>
0006        </ProtocolVersion>
0007        <BatchCount type="Integer" value="1"/>
0008      </RequestHeader>
0009      <BatchItem>
0010        <Operation type="Enumeration" value="Register"/>
0011        <RequestPayload>
0012          <ObjectType type="Enumeration" value="SymmetricKey"/>
0013          <TemplateAttribute>
0014            <Attribute>
0015              <AttributeName type="TextString" value="Cryptographic
        Usage Mask"/>
0016              <AttributeValue type="Integer" value="Encrypt Decrypt"/>
0017            </Attribute>
0018            <Attribute>
0019              <AttributeName type="TextString" value="x-ID"/>
0020              <AttributeValue type="TextString" value="CS-BC-M-6-12"/>
0021            </Attribute>
0022            <Attribute>
0023              <AttributeName type="TextString" value="Activation Date"/>
0024              <AttributeValue type="DateTime" value="$NOW-3600"/>
0025            </Attribute>
0026          </TemplateAttribute>
0027          <SymmetricKey>
0028            <KeyBlock>
0029              <KeyFormatType type="Enumeration" value="Raw"/>
0030              <KeyValue>
0031                <KeyMaterial type="ByteString"
        value="0123456789abcdef0123456789abcdef"/>
0032              </KeyValue>
0033              <CryptographicAlgorithm type="Enumeration" value="AES"/>
0034              <CryptographicLength type="Integer" value="128"/>
0035            </KeyBlock>
0036          </SymmetricKey>
```

```
0037      </RequestPayload>
0038    </BatchItem>
0039  </RequestMessage>
0040  <ResponseMessage>
0041    <ResponseHeader>
0042      <ProtocolVersion>
0043        <ProtocolVersionMajor type="Integer" value="1"/>
0044        <ProtocolVersionMinor type="Integer" value="2"/>
0045      </ProtocolVersion>
0046      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0047      <BatchCount type="Integer" value="1"/>
0048    </ResponseHeader>
0049    <BatchItem>
0050      <Operation type="Enumeration" value="Register"/>
0051      <ResultStatus type="Enumeration" value="Success"/>
0052      <ResponsePayload>
0053        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0054      </ResponsePayload>
0055    </BatchItem>
0056  </ResponseMessage>
      # TIME 1
0057  <RequestMessage>
0058    <RequestHeader>
0059      <ProtocolVersion>
0060        <ProtocolVersionMajor type="Integer" value="1"/>
0061        <ProtocolVersionMinor type="Integer" value="2"/>
0062      </ProtocolVersion>
0063      <BatchCount type="Integer" value="1"/>
0064    </RequestHeader>
0065    <BatchItem>
0066      <Operation type="Enumeration" value="Encrypt"/>
0067      <RequestPayload>
0068        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0069        <CryptographicParameters>
0070        <BlockCipherMode type="Enumeration" value="ECB"/>
0071        </CryptographicParameters>
0072        <Data type="ByteString"
      value="0102030405060708091011121314151 6"/>
0073      </RequestPayload>
0074    </BatchItem>
0075  </RequestMessage>
0076  <ResponseMessage>
0077    <ResponseHeader>
0078      <ProtocolVersion>
0079        <ProtocolVersionMajor type="Integer" value="1"/>
0080        <ProtocolVersionMinor type="Integer" value="2"/>
0081      </ProtocolVersion>
0082      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0083      <BatchCount type="Integer" value="1"/>
0084    </ResponseHeader>
0085    <BatchItem>
0086      <Operation type="Enumeration" value="Encrypt"/>
0087      <ResultStatus type="Enumeration" value="Success"/>
0088      <ResponsePayload>
0089        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
```

```
0090        <Data type="ByteString"
    value="fd912d102dbb482f6f6e91bd57119095"/>
0091      </ResponsePayload>
0092    </BatchItem>
0093  </ResponseMessage>
      # TIME 2
0094  <RequestMessage>
0095    <RequestHeader>
0096      <ProtocolVersion>
0097        <ProtocolVersionMajor type="Integer" value="1"/>
0098        <ProtocolVersionMinor type="Integer" value="2"/>
0099      </ProtocolVersion>
0100      <BatchCount type="Integer" value="1"/>
0101    </RequestHeader>
0102    <BatchItem>
0103      <Operation type="Enumeration" value="Decrypt"/>
0104      <RequestPayload>
0105        <UniqueIdentifier type="TextString"
    value="$UNIQUE_IDENTIFIER_0"/>
0106        <CryptographicParameters>
0107        <BlockCipherMode type="Enumeration" value="ECB"/>
0108        </CryptographicParameters>
0109        <Data type="ByteString"
    value="fd912d102dbb482f6f6e91bd57119095"/>
0110      </RequestPayload>
0111    </BatchItem>
0112  </RequestMessage>
0113  <ResponseMessage>
0114    <ResponseHeader>
0115      <ProtocolVersion>
0116        <ProtocolVersionMajor type="Integer" value="1"/>
0117        <ProtocolVersionMinor type="Integer" value="2"/>
0118      </ProtocolVersion>
0119      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0120      <BatchCount type="Integer" value="1"/>
0121    </ResponseHeader>
0122    <BatchItem>
0123      <Operation type="Enumeration" value="Decrypt"/>
0124      <ResultStatus type="Enumeration" value="Success"/>
0125      <ResponsePayload>
0126        <UniqueIdentifier type="TextString"
    value="$UNIQUE_IDENTIFIER_0"/>
0127        <Data type="ByteString"
    value="0102030405060708091011121314151 6"/>
0128      </ResponsePayload>
0129    </BatchItem>
0130  </ResponseMessage>
      # TIME 3
0131  <RequestMessage>
0132    <RequestHeader>
0133      <ProtocolVersion>
0134        <ProtocolVersionMajor type="Integer" value="1"/>
0135        <ProtocolVersionMinor type="Integer" value="2"/>
0136      </ProtocolVersion>
0137      <BatchCount type="Integer" value="1"/>
0138    </RequestHeader>
0139    <BatchItem>
0140      <Operation type="Enumeration" value="Revoke"/>
```

```
    <RequestPayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
      <RevocationReason>
        <RevocationReasonCode type="Enumeration"
value="Unspecified"/>
      </RevocationReason>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
    </ResponsePayload>
  </BatchItem>
</ResponseMessage>
```

```
# TIME 4
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
```

```
0194        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0195      </ResponsePayload>
0196    </BatchItem>
0197  </ResponseMessage>
```

136

137 3.1.7 CS-BC-M-7-12 - Encrypt with Known Symmetric Key with Usage Limits

138 Register a symmetric key and perform encrypt using the symmetric key. Then attempt to perform an
139 encrypt beyond the usage limits. It must fail. This is otherwise the same as CS-BC-M-4-12.

```
      # TIME 0
0001  <RequestMessage>
0002    <RequestHeader>
0003      <ProtocolVersion>
0004        <ProtocolVersionMajor type="Integer" value="1"/>
0005        <ProtocolVersionMinor type="Integer" value="2"/>
0006      </ProtocolVersion>
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="Register"/>
0011      <RequestPayload>
0012        <ObjectType type="Enumeration" value="SymmetricKey"/>
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
      Usage Mask"/>
0016            <AttributeValue type="Integer" value="Encrypt Decrypt"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="x-ID"/>
0020            <AttributeValue type="TextString" value="CS-BC-M-7-12"/>
0021          </Attribute>
0022          <Attribute>
0023            <AttributeName type="TextString" value="Activation Date"/>
0024            <AttributeValue type="DateTime" value="$NOW-3600"/>
0025          </Attribute>
0026        <Attribute>
0027          <AttributeName type="TextString" value="Usage Limits"/>
0028          <AttributeValue>
0029            <UsageLimitsTotal type="LongInteger" value="16"/>
0030            <UsageLimitsUnit type="Enumeration" value="Byte"/>
0031          </AttributeValue>
0032        </Attribute>
0033        </TemplateAttribute>
0034        <SymmetricKey>
0035          <KeyBlock>
0036            <KeyFormatType type="Enumeration" value="Raw"/>
0037            <KeyValue>
0038              <KeyMaterial type="ByteString"
      value="0123456789abcdef0123456789abcdef"/>
0039            </KeyValue>
0040            <CryptographicAlgorithm type="Enumeration" value="AES"/>
0041            <CryptographicLength type="Integer" value="128"/>
0042          </KeyBlock>
0043        </SymmetricKey>
```

```
0044        </RequestPayload>
0045      </BatchItem>
0046    </RequestMessage>
0047    <ResponseMessage>
0048      <ResponseHeader>
0049        <ProtocolVersion>
0050          <ProtocolVersionMajor type="Integer" value="1"/>
0051          <ProtocolVersionMinor type="Integer" value="2"/>
0052        </ProtocolVersion>
0053        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0054        <BatchCount type="Integer" value="1"/>
0055      </ResponseHeader>
0056      <BatchItem>
0057        <Operation type="Enumeration" value="Register"/>
0058        <ResultStatus type="Enumeration" value="Success"/>
0059        <ResponsePayload>
0060          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0061        </ResponsePayload>
0062      </BatchItem>
0063    </ResponseMessage>
          # TIME 1
0064    <RequestMessage>
0065      <RequestHeader>
0066        <ProtocolVersion>
0067          <ProtocolVersionMajor type="Integer" value="1"/>
0068          <ProtocolVersionMinor type="Integer" value="2"/>
0069        </ProtocolVersion>
0070        <BatchCount type="Integer" value="1"/>
0071      </RequestHeader>
0072      <BatchItem>
0073        <Operation type="Enumeration" value="Encrypt"/>
0074        <RequestPayload>
0075          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0076          <CryptographicParameters>
0077          <BlockCipherMode type="Enumeration" value="ECB"/>
0078          </CryptographicParameters>
0079          <Data type="ByteString"
          value="0102030405060708091011121314151 6"/>
0080        </RequestPayload>
0081      </BatchItem>
0082    </RequestMessage>
0083    <ResponseMessage>
0084      <ResponseHeader>
0085        <ProtocolVersion>
0086          <ProtocolVersionMajor type="Integer" value="1"/>
0087          <ProtocolVersionMinor type="Integer" value="2"/>
0088        </ProtocolVersion>
0089        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0090        <BatchCount type="Integer" value="1"/>
0091      </ResponseHeader>
0092      <BatchItem>
0093        <Operation type="Enumeration" value="Encrypt"/>
0094        <ResultStatus type="Enumeration" value="Success"/>
0095        <ResponsePayload>
0096          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
```

```
0097        <Data type="ByteString"
    value="d9bcce11b0b437b90239552df3a360c9"/>
0098      </ResponsePayload>
0099    </BatchItem>
0100  </ResponseMessage>
```

```
    # TIME 2
    # Attempt to protect beyond the usage limits. This must fail.
0101  <RequestMessage>
0102    <RequestHeader>
0103      <ProtocolVersion>
0104        <ProtocolVersionMajor type="Integer" value="1"/>
0105        <ProtocolVersionMinor type="Integer" value="2"/>
0106      </ProtocolVersion>
0107      <BatchCount type="Integer" value="1"/>
0108    </RequestHeader>
0109    <BatchItem>
0110      <Operation type="Enumeration" value="Encrypt"/>
0111      <RequestPayload>
0112        <UniqueIdentifier type="TextString"
    value="$UNIQUE_IDENTIFIER_0"/>
0113        <CryptographicParameters>
0114        <BlockCipherMode type="Enumeration" value="ECB"/>
0115        </CryptographicParameters>
0116        <Data type="ByteString"
    value="0102030405060708091011121314151 6"/>
0117      </RequestPayload>
0118    </BatchItem>
0119  </RequestMessage>
```

```
0120  <ResponseMessage>
0121    <ResponseHeader>
0122      <ProtocolVersion>
0123        <ProtocolVersionMajor type="Integer" value="1"/>
0124        <ProtocolVersionMinor type="Integer" value="2"/>
0125      </ProtocolVersion>
0126      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0127      <BatchCount type="Integer" value="1"/>
0128    </ResponseHeader>
0129    <BatchItem>
0130      <Operation type="Enumeration" value="Encrypt"/>
0131      <ResultStatus type="Enumeration" value="OperationFailed"/>
0132      <ResultReason type="Enumeration" value="PermissionDenied"/>
0133      <ResultMessage type="TextString" value="DENIED"/>
0134    </BatchItem>
0135  </ResponseMessage>
```

```
    # TIME 3
0136  <RequestMessage>
0137    <RequestHeader>
0138      <ProtocolVersion>
0139        <ProtocolVersionMajor type="Integer" value="1"/>
0140        <ProtocolVersionMinor type="Integer" value="2"/>
0141      </ProtocolVersion>
0142      <BatchCount type="Integer" value="1"/>
0143    </RequestHeader>
0144    <BatchItem>
0145      <Operation type="Enumeration" value="Revoke"/>
0146      <RequestPayload>
0147        <UniqueIdentifier type="TextString"
    value="$UNIQUE_IDENTIFIER_0"/>
```

```
0148        <RevocationReason>
0149          <RevocationReasonCode type="Enumeration"
      value="Unspecified"/>
0150        </RevocationReason>
0151      </RequestPayload>
0152    </BatchItem>
0153  </RequestMessage>
```

```
0154  <ResponseMessage>
0155    <ResponseHeader>
0156      <ProtocolVersion>
0157        <ProtocolVersionMajor type="Integer" value="1"/>
0158        <ProtocolVersionMinor type="Integer" value="2"/>
0159      </ProtocolVersion>
0160      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0161      <BatchCount type="Integer" value="1"/>
0162    </ResponseHeader>
0163    <BatchItem>
0164      <Operation type="Enumeration" value="Revoke"/>
0165      <ResultStatus type="Enumeration" value="Success"/>
0166      <ResponsePayload>
0167        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0168      </ResponsePayload>
0169    </BatchItem>
0170  </ResponseMessage>
```

```
      # TIME 4
0171  <RequestMessage>
0172    <RequestHeader>
0173      <ProtocolVersion>
0174        <ProtocolVersionMajor type="Integer" value="1"/>
0175        <ProtocolVersionMinor type="Integer" value="2"/>
0176      </ProtocolVersion>
0177      <BatchCount type="Integer" value="1"/>
0178    </RequestHeader>
0179    <BatchItem>
0180      <Operation type="Enumeration" value="Destroy"/>
0181      <RequestPayload>
0182        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0183      </RequestPayload>
0184    </BatchItem>
0185  </RequestMessage>
```

```
0186  <ResponseMessage>
0187    <ResponseHeader>
0188      <ProtocolVersion>
0189        <ProtocolVersionMajor type="Integer" value="1"/>
0190        <ProtocolVersionMinor type="Integer" value="2"/>
0191      </ProtocolVersion>
0192      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0193      <BatchCount type="Integer" value="1"/>
0194    </ResponseHeader>
0195    <BatchItem>
0196      <Operation type="Enumeration" value="Destroy"/>
0197      <ResultStatus type="Enumeration" value="Success"/>
0198      <ResponsePayload>
0199        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0200      </ResponsePayload>
```

```
0201    </BatchItem>
0202  </ResponseMessage>
```

140

141 3.1.8 CS-BC-M-8-12 - Encrypt and Decrypt with Known Symmetric Key and
142 PKCS5 Padding

143 Register a symmetric key and perform encrypt using the symmetric key followed by decrypt. This is
144 otherwise the same as CS-BC-M-3-12.

```
      # TIME 0
0001  <RequestMessage>
0002    <RequestHeader>
0003      <ProtocolVersion>
0004        <ProtocolVersionMajor type="Integer" value="1"/>
0005        <ProtocolVersionMinor type="Integer" value="2"/>
0006      </ProtocolVersion>
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="Register"/>
0011      <RequestPayload>
0012        <ObjectType type="Enumeration" value="SymmetricKey"/>
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
      Usage Mask"/>
0016            <AttributeValue type="Integer" value="Encrypt Decrypt"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="x-ID"/>
0020            <AttributeValue type="TextString" value="CS-BC-M-8-12"/>
0021          </Attribute>
0022          <Attribute>
0023            <AttributeName type="TextString" value="Activation Date"/>
0024            <AttributeValue type="DateTime" value="$NOW-3600"/>
0025          </Attribute>
0026        </TemplateAttribute>
0027        <SymmetricKey>
0028          <KeyBlock>
0029            <KeyFormatType type="Enumeration" value="Raw"/>
0030            <KeyValue>
0031              <KeyMaterial type="ByteString"
      value="0123456789abcdef0123456789abcdef"/>
0032            </KeyValue>
0033            <CryptographicAlgorithm type="Enumeration" value="AES"/>
0034            <CryptographicLength type="Integer" value="128"/>
0035          </KeyBlock>
0036        </SymmetricKey>
0037      </RequestPayload>
0038    </BatchItem>
0039  </RequestMessage>
```

```
0040  <ResponseMessage>
0041    <ResponseHeader>
0042      <ProtocolVersion>
0043        <ProtocolVersionMajor type="Integer" value="1"/>
0044        <ProtocolVersionMinor type="Integer" value="2"/>
0045      </ProtocolVersion>
```

```
0046        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0047        <BatchCount type="Integer" value="1"/>
0048      </ResponseHeader>
0049      <BatchItem>
0050        <Operation type="Enumeration" value="Register"/>
0051        <ResultStatus type="Enumeration" value="Success"/>
0052        <ResponsePayload>
0053          <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0054        </ResponsePayload>
0055      </BatchItem>
0056    </ResponseMessage>
```

```
          # TIME 1
0057    <RequestMessage>
0058      <RequestHeader>
0059        <ProtocolVersion>
0060          <ProtocolVersionMajor type="Integer" value="1"/>
0061          <ProtocolVersionMinor type="Integer" value="2"/>
0062        </ProtocolVersion>
0063        <BatchCount type="Integer" value="1"/>
0064      </RequestHeader>
0065      <BatchItem>
0066        <Operation type="Enumeration" value="Encrypt"/>
0067        <RequestPayload>
0068          <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0069          <CryptographicParameters>
0070          <BlockCipherMode type="Enumeration" value="ECB"/>
0071          <PaddingMethod type="Enumeration" value="PKCS5"/>
0072          </CryptographicParameters>
0073          <Data type="ByteString"
      value="0102030405060708091011121314151 6"/>
0074        </RequestPayload>
0075      </BatchItem>
0076    </RequestMessage>
```

```
0077    <ResponseMessage>
0078      <ResponseHeader>
0079        <ProtocolVersion>
0080          <ProtocolVersionMajor type="Integer" value="1"/>
0081          <ProtocolVersionMinor type="Integer" value="2"/>
0082        </ProtocolVersion>
0083        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0084        <BatchCount type="Integer" value="1"/>
0085      </ResponseHeader>
0086      <BatchItem>
0087        <Operation type="Enumeration" value="Encrypt"/>
0088        <ResultStatus type="Enumeration" value="Success"/>
0089        <ResponsePayload>
0090          <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0091          <Data type="ByteString"
      value="d9bcce11b0b437b90239552df3a360c90efb6bfed93b4d1ea2123ba4db075
      ff6"/>
0092        </ResponsePayload>
0093      </BatchItem>
0094    </ResponseMessage>
```

```
          # TIME 2
0095    <RequestMessage>
```

```
0096    <RequestHeader>
0097      <ProtocolVersion>
0098        <ProtocolVersionMajor type="Integer" value="1"/>
0099        <ProtocolVersionMinor type="Integer" value="2"/>
0100      </ProtocolVersion>
0101      <BatchCount type="Integer" value="1"/>
0102    </RequestHeader>
0103    <BatchItem>
0104      <Operation type="Enumeration" value="Decrypt"/>
0105      <RequestPayload>
0106        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0107        <CryptographicParameters>
0108        <BlockCipherMode type="Enumeration" value="ECB"/>
0109        <PaddingMethod type="Enumeration" value="PKCS5"/>
0110        </CryptographicParameters>
0111        <Data type="ByteString"
        value="d9bcce11b0b437b90239552df3a360c90efb6bfed93b4d1ea2123ba4db075
        ff6"/>
0112      </RequestPayload>
0113    </BatchItem>
0114  </RequestMessage>
```

```
0115  <ResponseMessage>
0116    <ResponseHeader>
0117      <ProtocolVersion>
0118        <ProtocolVersionMajor type="Integer" value="1"/>
0119        <ProtocolVersionMinor type="Integer" value="2"/>
0120      </ProtocolVersion>
0121      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0122      <BatchCount type="Integer" value="1"/>
0123    </ResponseHeader>
0124    <BatchItem>
0125      <Operation type="Enumeration" value="Decrypt"/>
0126      <ResultStatus type="Enumeration" value="Success"/>
0127      <ResponsePayload>
0128        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0129        <Data type="ByteString"
        value="0102030405060708091011121314151 6"/>
0130      </ResponsePayload>
0131    </BatchItem>
0132  </ResponseMessage>
```

```
        # TIME 3
0133  <RequestMessage>
0134    <RequestHeader>
0135      <ProtocolVersion>
0136        <ProtocolVersionMajor type="Integer" value="1"/>
0137        <ProtocolVersionMinor type="Integer" value="2"/>
0138      </ProtocolVersion>
0139      <BatchCount type="Integer" value="1"/>
0140    </RequestHeader>
0141    <BatchItem>
0142      <Operation type="Enumeration" value="Revoke"/>
0143      <RequestPayload>
0144        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0145        <RevocationReason>
0146          <RevocationReasonCode type="Enumeration"
```

```
      value="Unspecified"/>
0147        </RevocationReason>
0148      </RequestPayload>
0149    </BatchItem>
0150  </RequestMessage>
0151  <ResponseMessage>
0152    <ResponseHeader>
0153      <ProtocolVersion>
0154        <ProtocolVersionMajor type="Integer" value="1"/>
0155        <ProtocolVersionMinor type="Integer" value="2"/>
0156      </ProtocolVersion>
0157      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0158      <BatchCount type="Integer" value="1"/>
0159    </ResponseHeader>
0160    <BatchItem>
0161      <Operation type="Enumeration" value="Revoke"/>
0162      <ResultStatus type="Enumeration" value="Success"/>
0163      <ResponsePayload>
0164        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0165      </ResponsePayload>
0166    </BatchItem>
0167  </ResponseMessage>
      # TIME 4
0168  <RequestMessage>
0169    <RequestHeader>
0170      <ProtocolVersion>
0171        <ProtocolVersionMajor type="Integer" value="1"/>
0172        <ProtocolVersionMinor type="Integer" value="2"/>
0173      </ProtocolVersion>
0174      <BatchCount type="Integer" value="1"/>
0175    </RequestHeader>
0176    <BatchItem>
0177      <Operation type="Enumeration" value="Destroy"/>
0178      <RequestPayload>
0179        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0180      </RequestPayload>
0181    </BatchItem>
0182  </RequestMessage>
0183  <ResponseMessage>
0184    <ResponseHeader>
0185      <ProtocolVersion>
0186        <ProtocolVersionMajor type="Integer" value="1"/>
0187        <ProtocolVersionMinor type="Integer" value="2"/>
0188      </ProtocolVersion>
0189      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0190      <BatchCount type="Integer" value="1"/>
0191    </ResponseHeader>
0192    <BatchItem>
0193      <Operation type="Enumeration" value="Destroy"/>
0194      <ResultStatus type="Enumeration" value="Success"/>
0195      <ResponsePayload>
0196        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0197      </ResponsePayload>
0198    </BatchItem>
0199  </ResponseMessage>
```

3.1.9 CS-BC-M-9-12 - Encrypt and Decrypt with Known Symmetric Key and PKCS5 Padding

Register a symmetric key and perform encrypt using the symmetric key followed by decrypt. The input data is non-block size. This is otherwise the same as CS-BC-M-8-12.

```
        # TIME 0
0001    <RequestMessage>
0002      <RequestHeader>
0003        <ProtocolVersion>
0004          <ProtocolVersionMajor type="Integer" value="1"/>
0005          <ProtocolVersionMinor type="Integer" value="2"/>
0006        </ProtocolVersion>
0007        <BatchCount type="Integer" value="1"/>
0008      </RequestHeader>
0009      <BatchItem>
0010        <Operation type="Enumeration" value="Register"/>
0011        <RequestPayload>
0012          <ObjectType type="Enumeration" value="SymmetricKey"/>
0013          <TemplateAttribute>
0014            <Attribute>
0015              <AttributeName type="TextString" value="Cryptographic
    Usage Mask"/>
0016              <AttributeValue type="Integer" value="Encrypt Decrypt"/>
0017            </Attribute>
0018            <Attribute>
0019              <AttributeName type="TextString" value="x-ID"/>
0020              <AttributeValue type="TextString" value="CS-BC-M-9-12"/>
0021            </Attribute>
0022            <Attribute>
0023              <AttributeName type="TextString" value="Activation Date"/>
0024              <AttributeValue type="DateTime" value="$NOW-3600"/>
0025            </Attribute>
0026          </TemplateAttribute>
0027          <SymmetricKey>
0028            <KeyBlock>
0029              <KeyFormatType type="Enumeration" value="Raw"/>
0030              <KeyValue>
0031                <KeyMaterial type="ByteString"
    value="0123456789abcdef0123456789abcdef"/>
0032              </KeyValue>
0033              <CryptographicAlgorithm type="Enumeration" value="AES"/>
0034              <CryptographicLength type="Integer" value="128"/>
0035            </KeyBlock>
0036          </SymmetricKey>
0037        </RequestPayload>
0038      </BatchItem>
0039    </RequestMessage>
0040    <ResponseMessage>
0041      <ResponseHeader>
0042        <ProtocolVersion>
0043          <ProtocolVersionMajor type="Integer" value="1"/>
0044          <ProtocolVersionMinor type="Integer" value="2"/>
0045        </ProtocolVersion>
0046        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0047        <BatchCount type="Integer" value="1"/>
```

```
0048    </ResponseHeader>
0049    <BatchItem>
0050      <Operation type="Enumeration" value="Register"/>
0051      <ResultStatus type="Enumeration" value="Success"/>
0052      <ResponsePayload>
0053        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0054      </ResponsePayload>
0055    </BatchItem>
0056  </ResponseMessage>
```

```
      # TIME 1
0057  <RequestMessage>
0058    <RequestHeader>
0059      <ProtocolVersion>
0060        <ProtocolVersionMajor type="Integer" value="1"/>
0061        <ProtocolVersionMinor type="Integer" value="2"/>
0062      </ProtocolVersion>
0063      <BatchCount type="Integer" value="1"/>
0064    </RequestHeader>
0065    <BatchItem>
0066      <Operation type="Enumeration" value="Encrypt"/>
0067      <RequestPayload>
0068        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0069        <CryptographicParameters>
0070        <BlockCipherMode type="Enumeration" value="ECB"/>
0071        <PaddingMethod type="Enumeration" value="PKCS5"/>
0072        </CryptographicParameters>
0073        <Data type="ByteString"
      value="0102030405060708091011121314151601020304050607080910111213141
      51601"/>
0074      </RequestPayload>
0075    </BatchItem>
0076  </RequestMessage>
```

```
0077  <ResponseMessage>
0078    <ResponseHeader>
0079      <ProtocolVersion>
0080        <ProtocolVersionMajor type="Integer" value="1"/>
0081        <ProtocolVersionMinor type="Integer" value="2"/>
0082      </ProtocolVersion>
0083      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0084      <BatchCount type="Integer" value="1"/>
0085    </ResponseHeader>
0086    <BatchItem>
0087      <Operation type="Enumeration" value="Encrypt"/>
0088      <ResultStatus type="Enumeration" value="Success"/>
0089      <ResponsePayload>
0090        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0091        <Data type="ByteString"
      value="d9bcce11b0b437b90239552df3a360c9d9bcce11b0b437b90239552df3a36
      0c9be261a7bd1371bb738fe004d500381d0"/>
0092      </ResponsePayload>
0093    </BatchItem>
0094  </ResponseMessage>
```

```
      # TIME 2
0095  <RequestMessage>
0096    <RequestHeader>
```

```
0097        <ProtocolVersion>
0098          <ProtocolVersionMajor type="Integer" value="1"/>
0099          <ProtocolVersionMinor type="Integer" value="2"/>
0100        </ProtocolVersion>
0101        <BatchCount type="Integer" value="1"/>
0102      </RequestHeader>
0103      <BatchItem>
0104        <Operation type="Enumeration" value="Decrypt"/>
0105        <RequestPayload>
0106          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0107          <CryptographicParameters>
0108          <BlockCipherMode type="Enumeration" value="ECB"/>
0109          <PaddingMethod type="Enumeration" value="PKCS5"/>
0110          </CryptographicParameters>
0111          <Data type="ByteString"
          value="d9bcce11b0b437b90239552df3a360c9d9bcce11b0b437b90239552df3a36
          0c9be261a7bd1371bb738fe004d500381d0"/>
0112        </RequestPayload>
0113      </BatchItem>
0114    </RequestMessage>
```

```
0115    <ResponseMessage>
0116      <ResponseHeader>
0117        <ProtocolVersion>
0118          <ProtocolVersionMajor type="Integer" value="1"/>
0119          <ProtocolVersionMinor type="Integer" value="2"/>
0120        </ProtocolVersion>
0121        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0122        <BatchCount type="Integer" value="1"/>
0123      </ResponseHeader>
0124      <BatchItem>
0125        <Operation type="Enumeration" value="Decrypt"/>
0126        <ResultStatus type="Enumeration" value="Success"/>
0127        <ResponsePayload>
0128          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0129          <Data type="ByteString"
          value="0102030405060708091011121314151601020304050607080910111213141
          51601"/>
0130        </ResponsePayload>
0131      </BatchItem>
0132    </ResponseMessage>
```

```
          # TIME 3
0133    <RequestMessage>
0134      <RequestHeader>
0135        <ProtocolVersion>
0136          <ProtocolVersionMajor type="Integer" value="1"/>
0137          <ProtocolVersionMinor type="Integer" value="2"/>
0138        </ProtocolVersion>
0139        <BatchCount type="Integer" value="1"/>
0140      </RequestHeader>
0141      <BatchItem>
0142        <Operation type="Enumeration" value="Revoke"/>
0143        <RequestPayload>
0144          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0145          <RevocationReason>
0146            <RevocationReasonCode type="Enumeration"
```

```
value="Unspecified"/>
0147        </RevocationReason>
0148      </RequestPayload>
0149    </BatchItem>
0150  </RequestMessage>
0151  <ResponseMessage>
0152    <ResponseHeader>
0153      <ProtocolVersion>
0154        <ProtocolVersionMajor type="Integer" value="1"/>
0155        <ProtocolVersionMinor type="Integer" value="2"/>
0156      </ProtocolVersion>
0157      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0158      <BatchCount type="Integer" value="1"/>
0159    </ResponseHeader>
0160    <BatchItem>
0161      <Operation type="Enumeration" value="Revoke"/>
0162      <ResultStatus type="Enumeration" value="Success"/>
0163      <ResponsePayload>
0164        <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0165      </ResponsePayload>
0166    </BatchItem>
0167  </ResponseMessage>
    # TIME 4
0168  <RequestMessage>
0169    <RequestHeader>
0170      <ProtocolVersion>
0171        <ProtocolVersionMajor type="Integer" value="1"/>
0172        <ProtocolVersionMinor type="Integer" value="2"/>
0173      </ProtocolVersion>
0174      <BatchCount type="Integer" value="1"/>
0175    </RequestHeader>
0176    <BatchItem>
0177      <Operation type="Enumeration" value="Destroy"/>
0178      <RequestPayload>
0179        <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0180      </RequestPayload>
0181    </BatchItem>
0182  </RequestMessage>
0183  <ResponseMessage>
0184    <ResponseHeader>
0185      <ProtocolVersion>
0186        <ProtocolVersionMajor type="Integer" value="1"/>
0187        <ProtocolVersionMinor type="Integer" value="2"/>
0188      </ProtocolVersion>
0189      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0190      <BatchCount type="Integer" value="1"/>
0191    </ResponseHeader>
0192    <BatchItem>
0193      <Operation type="Enumeration" value="Destroy"/>
0194      <ResultStatus type="Enumeration" value="Success"/>
0195      <ResponsePayload>
0196        <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0197      </ResponsePayload>
0198    </BatchItem>
0199  </ResponseMessage>
```

3.1.10 CS-BC-M-10-12 - Encrypt and Decrypt with Known Symmetric Key and PKCS5 Padding and CBC

Register a symmetric key and perform encrypt using the symmetric key followed by decrypt. The input data is non-block size. This is otherwise the same as CS-BC-M-9-12.

```
        # TIME 0
0001    <RequestMessage>
0002      <RequestHeader>
0003        <ProtocolVersion>
0004          <ProtocolVersionMajor type="Integer" value="1"/>
0005          <ProtocolVersionMinor type="Integer" value="2"/>
0006        </ProtocolVersion>
0007        <BatchCount type="Integer" value="1"/>
0008      </RequestHeader>
0009      <BatchItem>
0010        <Operation type="Enumeration" value="Register"/>
0011        <RequestPayload>
0012          <ObjectType type="Enumeration" value="SymmetricKey"/>
0013          <TemplateAttribute>
0014            <Attribute>
0015              <AttributeName type="TextString" value="Cryptographic
    Usage Mask"/>
0016              <AttributeValue type="Integer" value="Encrypt Decrypt"/>
0017            </Attribute>
0018            <Attribute>
0019              <AttributeName type="TextString" value="x-ID"/>
0020              <AttributeValue type="TextString" value="CS-BC-M-10-12"/>
0021            </Attribute>
0022            <Attribute>
0023              <AttributeName type="TextString" value="Activation Date"/>
0024              <AttributeValue type="DateTime" value="$NOW-3600"/>
0025            </Attribute>
0026          </TemplateAttribute>
0027          <SymmetricKey>
0028            <KeyBlock>
0029              <KeyFormatType type="Enumeration" value="Raw"/>
0030              <KeyValue>
0031                <KeyMaterial type="ByteString"
    value="0123456789abcdef0123456789abcdef"/>
0032              </KeyValue>
0033              <CryptographicAlgorithm type="Enumeration" value="AES"/>
0034              <CryptographicLength type="Integer" value="128"/>
0035            </KeyBlock>
0036          </SymmetricKey>
0037        </RequestPayload>
0038      </BatchItem>
0039    </RequestMessage>
0040    <ResponseMessage>
0041      <ResponseHeader>
0042        <ProtocolVersion>
0043          <ProtocolVersionMajor type="Integer" value="1"/>
0044          <ProtocolVersionMinor type="Integer" value="2"/>
0045        </ProtocolVersion>
0046        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0047        <BatchCount type="Integer" value="1"/>
```

```
0048    </ResponseHeader>
0049    <BatchItem>
0050      <Operation type="Enumeration" value="Register"/>
0051      <ResultStatus type="Enumeration" value="Success"/>
0052      <ResponsePayload>
0053        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0054      </ResponsePayload>
0055    </BatchItem>
0056  </ResponseMessage>
```

```
        # TIME 1
0057  <RequestMessage>
0058    <RequestHeader>
0059      <ProtocolVersion>
0060        <ProtocolVersionMajor type="Integer" value="1"/>
0061        <ProtocolVersionMinor type="Integer" value="2"/>
0062      </ProtocolVersion>
0063      <BatchCount type="Integer" value="1"/>
0064    </RequestHeader>
0065    <BatchItem>
0066      <Operation type="Enumeration" value="Encrypt"/>
0067      <RequestPayload>
0068        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0069        <CryptographicParameters>
0070        <BlockCipherMode type="Enumeration" value="CBC"/>
0071        <PaddingMethod type="Enumeration" value="PKCS5"/>
0072        </CryptographicParameters>
0073        <Data type="ByteString"
        value="0102030405060708091011121314151601020304050607080910111213141
        51601"/>
0074        <IVCounterNonce type="ByteString"
        value="01020304050607080910111213141516"/>
0075      </RequestPayload>
0076    </BatchItem>
0077  </RequestMessage>
```

```
0078  <ResponseMessage>
0079    <ResponseHeader>
0080      <ProtocolVersion>
0081        <ProtocolVersionMajor type="Integer" value="1"/>
0082        <ProtocolVersionMinor type="Integer" value="2"/>
0083      </ProtocolVersion>
0084      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0085      <BatchCount type="Integer" value="1"/>
0086    </ResponseHeader>
0087    <BatchItem>
0088      <Operation type="Enumeration" value="Encrypt"/>
0089      <ResultStatus type="Enumeration" value="Success"/>
0090      <ResponsePayload>
0091        <UniqueIdentifier type="TextString"
        value="$UNIQUE IDENTIFIER 0"/>
0092        <Data type="ByteString"
        value="79abc5c23868ad84d388ce61110a62742bda19d694bbcb757dd06617c0d80
        fb1df2e71864ad9633d7d797e30860df00d"/>
0093      </ResponsePayload>
0094    </BatchItem>
0095  </ResponseMessage>
```

```
        # TIME 2
```

```
0096 <RequestMessage>
0097   <RequestHeader>
0098     <ProtocolVersion>
0099       <ProtocolVersionMajor type="Integer" value="1"/>
0100       <ProtocolVersionMinor type="Integer" value="2"/>
0101     </ProtocolVersion>
0102     <BatchCount type="Integer" value="1"/>
0103   </RequestHeader>
0104   <BatchItem>
0105     <Operation type="Enumeration" value="Decrypt"/>
0106     <RequestPayload>
0107       <UniqueIdentifier type="TextString"
       value="$UNIQUE_IDENTIFIER_0"/>
0108       <CryptographicParameters>
0109       <BlockCipherMode type="Enumeration" value="CBC"/>
0110       <PaddingMethod type="Enumeration" value="PKCS5"/>
0111       </CryptographicParameters>
0112       <Data type="ByteString"
       value="79abc5c23868ad84d388ce61110a62742bda19d694bbcb757dd06617c0d80
       fb1df2e71864ad9633d7d797e30860df00d"/>
0113       <IVCounterNonce type="ByteString"
       value="0102030405060708091011121314151 6"/>
0114     </RequestPayload>
0115   </BatchItem>
0116 </RequestMessage>
```

```
0117 <ResponseMessage>
0118   <ResponseHeader>
0119     <ProtocolVersion>
0120       <ProtocolVersionMajor type="Integer" value="1"/>
0121       <ProtocolVersionMinor type="Integer" value="2"/>
0122     </ProtocolVersion>
0123     <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0124     <BatchCount type="Integer" value="1"/>
0125   </ResponseHeader>
0126   <BatchItem>
0127     <Operation type="Enumeration" value="Decrypt"/>
0128     <ResultStatus type="Enumeration" value="Success"/>
0129     <ResponsePayload>
0130       <UniqueIdentifier type="TextString"
       value="$UNIQUE_IDENTIFIER_0"/>
0131       <Data type="ByteString"
       value="0102030405060708091011121314151601020304050607080910111213141
       51601"/>
0132     </ResponsePayload>
0133   </BatchItem>
0134 </ResponseMessage>
```

```
       # TIME 3
0135 <RequestMessage>
0136   <RequestHeader>
0137     <ProtocolVersion>
0138       <ProtocolVersionMajor type="Integer" value="1"/>
0139       <ProtocolVersionMinor type="Integer" value="2"/>
0140     </ProtocolVersion>
0141     <BatchCount type="Integer" value="1"/>
0142   </RequestHeader>
0143   <BatchItem>
0144     <Operation type="Enumeration" value="Revoke"/>
0145     <RequestPayload>
```

```
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
      <RevocationReason>
        <RevocationReasonCode type="Enumeration"
value="Unspecified"/>
      </RevocationReason>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
    </ResponsePayload>
  </BatchItem>
</ResponseMessage>
```

```
# TIME 4
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString"
```

```
      value="$UNIQUE_IDENTIFIER_0"/>
0199      </ResponsePayload>
0200    </BatchItem>
0201  </ResponseMessage>
```

155

156 3.1.11 CS-BC-M-11-12 - Encrypt and Decrypt with Known Symmetric Key
157 and PKCS5 Padding and CBC and IV

158 Register a symmetric key and perform encrypt using the symmetric key followed by decrypt. The input
159 data is non-block size. This is otherwise the same as CS-BC-M-10-12.

```
      # TIME 0
0001  <RequestMessage>
0002    <RequestHeader>
0003      <ProtocolVersion>
0004        <ProtocolVersionMajor type="Integer" value="1"/>
0005        <ProtocolVersionMinor type="Integer" value="2"/>
0006      </ProtocolVersion>
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="Register"/>
0011      <RequestPayload>
0012        <ObjectType type="Enumeration" value="SymmetricKey"/>
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
      Usage Mask"/>
0016            <AttributeValue type="Integer" value="Encrypt Decrypt"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="x-ID"/>
0020            <AttributeValue type="TextString" value="CS-BC-M-11-12"/>
0021          </Attribute>
0022          <Attribute>
0023            <AttributeName type="TextString" value="Activation Date"/>
0024            <AttributeValue type="DateTime" value="$NOW-3600"/>
0025          </Attribute>
0026        </TemplateAttribute>
0027        <SymmetricKey>
0028          <KeyBlock>
0029            <KeyFormatType type="Enumeration" value="Raw"/>
0030            <KeyValue>
0031              <KeyMaterial type="ByteString"
      value="0123456789abcdef0123456789abcdef"/>
0032            </KeyValue>
0033            <CryptographicAlgorithm type="Enumeration" value="AES"/>
0034            <CryptographicLength type="Integer" value="128"/>
0035          </KeyBlock>
0036        </SymmetricKey>
0037      </RequestPayload>
0038    </BatchItem>
0039  </RequestMessage>
```

```
0040  <ResponseMessage>
0041    <ResponseHeader>
0042      <ProtocolVersion>
0043        <ProtocolVersionMajor type="Integer" value="1"/>
```

```
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Register"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
    </ResponsePayload>
  </BatchItem>
</ResponseMessage>
```

```
# TIME 1
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Encrypt"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
      <CryptographicParameters>
      <BlockCipherMode type="Enumeration" value="CBC"/>
      <PaddingMethod type="Enumeration" value="PKCS5"/>
      </CryptographicParameters>
      <Data type="ByteString"
value="0102030405060708091011121314151601020304050607080910111213141
51601"/>
      <IVCounterNonce type="ByteString"
value="FF02030405060708091011121314151 6"/>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Encrypt"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
      <Data type="ByteString"
value="e768203ba72b6e157daaad34b1e791d8e88457dc147942f01bfaff7b28a3c
dde2203d4d5a4c7928ba9e9cc78b66a6546"/>
```

```
0093        </ResponsePayload>
0094      </BatchItem>
0095    </ResponseMessage>
        # TIME 2
        # Decrypt with the IV being specified as all zeros (which does
        # not match the Encrypt) will result in the first block being
        # incorrect.
0096    <RequestMessage>
0097      <RequestHeader>
0098        <ProtocolVersion>
0099          <ProtocolVersionMajor type="Integer" value="1"/>
0100          <ProtocolVersionMinor type="Integer" value="2"/>
0101        </ProtocolVersion>
0102        <BatchCount type="Integer" value="1"/>
0103      </RequestHeader>
0104      <BatchItem>
0105        <Operation type="Enumeration" value="Decrypt"/>
0106        <RequestPayload>
0107          <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0108          <CryptographicParameters>
0109          <BlockCipherMode type="Enumeration" value="CBC"/>
0110          <PaddingMethod type="Enumeration" value="PKCS5"/>
0111          </CryptographicParameters>
0112          <Data type="ByteString"
        value="e768203ba72b6e157daaad34b1e791d8e88457dc147942f01bfaff7b28a3c
        dde2203d4d5a4c7928ba9e9cc78b66a6546"/>
0113          <IVCounterNonce type="ByteString"
        value="00000000000000000000000000000000"/>
0114        </RequestPayload>
0115      </BatchItem>
0116    </RequestMessage>
0117    <ResponseMessage>
0118      <ResponseHeader>
0119        <ProtocolVersion>
0120          <ProtocolVersionMajor type="Integer" value="1"/>
0121          <ProtocolVersionMinor type="Integer" value="2"/>
0122        </ProtocolVersion>
0123        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0124        <BatchCount type="Integer" value="1"/>
0125      </ResponseHeader>
0126      <BatchItem>
0127        <Operation type="Enumeration" value="Decrypt"/>
0128        <ResultStatus type="Enumeration" value="Success"/>
0129        <ResponsePayload>
0130          <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0131          <Data type="ByteString"
        value="fe000000000000000000000000000000010203040506070809101112131415
        1601"/>
0132        </ResponsePayload>
0133      </BatchItem>
0134    </ResponseMessage>
        # TIME 3
        # Decrypt without the IV being specified will result in an error
0135    <RequestMessage>
0136      <RequestHeader>
0137        <ProtocolVersion>
```

```
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Decrypt"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
      <CryptographicParameters>
      <BlockCipherMode type="Enumeration" value="CBC"/>
      <PaddingMethod type="Enumeration" value="PKCS5"/>
      </CryptographicParameters>
      <Data type="ByteString"
value="e768203ba72b6e157daaad34b1e791d8e88457dc147942f01bfaff7b28a3c
dde2203d4d5a4c7928ba9e9cc78b66a6546"/>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Decrypt"/>
    <ResultStatus type="Enumeration" value="OperationFailed"/>
    <ResultReason type="Enumeration" value="InvalidMessage"/>
    <ResultMessage type="TextString" value="missing-iv"/>
  </BatchItem>
</ResponseMessage>
```

```
# TIME 4
# Decrypt with the IV being specified
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Decrypt"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
      <CryptographicParameters>
      <BlockCipherMode type="Enumeration" value="CBC"/>
      <PaddingMethod type="Enumeration" value="PKCS5"/>
      </CryptographicParameters>
      <Data type="ByteString"
value="e768203ba72b6e157daaad34b1e791d8e88457dc147942f01bfaff7b28a3c
dde2203d4d5a4c7928ba9e9cc78b66a6546"/>
```

```
      <IVCounterNonce type="ByteString"
value="FF020304050607080910111213141516"/>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Decrypt"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
      <Data type="ByteString"
value="0102030405060708091011121314151601020304050607080910111213141
51601"/>
    </ResponsePayload>
  </BatchItem>
</ResponseMessage>
```

```
# TIME 5
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
      <RevocationReason>
        <RevocationReasonCode type="Enumeration"
value="Unspecified"/>
      </RevocationReason>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
```

```
0239      <ResultStatus type="Enumeration" value="Success"/>
0240      <ResponsePayload>
0241        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0242      </ResponsePayload>
0243    </BatchItem>
0244  </ResponseMessage>
```

```
          # TIME 6
0245  <RequestMessage>
0246    <RequestHeader>
0247      <ProtocolVersion>
0248        <ProtocolVersionMajor type="Integer" value="1"/>
0249        <ProtocolVersionMinor type="Integer" value="2"/>
0250      </ProtocolVersion>
0251      <BatchCount type="Integer" value="1"/>
0252    </RequestHeader>
0253    <BatchItem>
0254      <Operation type="Enumeration" value="Destroy"/>
0255      <RequestPayload>
0256        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0257      </RequestPayload>
0258    </BatchItem>
0259  </RequestMessage>
```

```
0260  <ResponseMessage>
0261    <ResponseHeader>
0262      <ProtocolVersion>
0263        <ProtocolVersionMajor type="Integer" value="1"/>
0264        <ProtocolVersionMinor type="Integer" value="2"/>
0265      </ProtocolVersion>
0266      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0267      <BatchCount type="Integer" value="1"/>
0268    </ResponseHeader>
0269    <BatchItem>
0270      <Operation type="Enumeration" value="Destroy"/>
0271      <ResultStatus type="Enumeration" value="Success"/>
0272      <ResponsePayload>
0273        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0274      </ResponsePayload>
0275    </BatchItem>
0276  </ResponseMessage>
```

160

161 ### 3.1.12 CS-BC-M-12-12 - Encrypt and Decrypt with Known Symmetric Key
162 ### and PKCS5 Padding and CBC and IV

163 Register a symmetric key and perform encrypt using the symmetric key followed by decrypt. The input
164 data is non-block size. The Cryptographic Parameters are associated attributes of the key rather than
165 parameters to the operation. This is otherwise the same as CS-BC-M-11-12.

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

```
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="Register"/>
0011      <RequestPayload>
0012        <ObjectType type="Enumeration" value="SymmetricKey"/>
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
    Usage Mask"/>
0016            <AttributeValue type="Integer" value="Encrypt Decrypt"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="x-ID"/>
0020            <AttributeValue type="TextString" value="CS-BC-M-12-12"/>
0021          </Attribute>
0022          <Attribute>
0023            <AttributeName type="TextString" value="Activation Date"/>
0024            <AttributeValue type="DateTime" value="$NOW-3600"/>
0025          </Attribute>
0026          <Attribute>
0027            <AttributeName type="TextString" value="Cryptographic
    Parameters"/>
0028          <AttributeValue>
0029            <BlockCipherMode type="Enumeration" value="CBC"/>
0030            <PaddingMethod type="Enumeration" value="PKCS5"/>
0031          </AttributeValue>
0032          </Attribute>
0033        </TemplateAttribute>
0034        <SymmetricKey>
0035          <KeyBlock>
0036            <KeyFormatType type="Enumeration" value="Raw"/>
0037            <KeyValue>
0038              <KeyMaterial type="ByteString"
    value="0123456789abcdef0123456789abcdef"/>
0039            </KeyValue>
0040            <CryptographicAlgorithm type="Enumeration" value="AES"/>
0041            <CryptographicLength type="Integer" value="128"/>
0042          </KeyBlock>
0043        </SymmetricKey>
0044      </RequestPayload>
0045    </BatchItem>
0046  </RequestMessage>
```

```
0047  <ResponseMessage>
0048    <ResponseHeader>
0049      <ProtocolVersion>
0050        <ProtocolVersionMajor type="Integer" value="1"/>
0051        <ProtocolVersionMinor type="Integer" value="2"/>
0052      </ProtocolVersion>
0053      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0054      <BatchCount type="Integer" value="1"/>
0055    </ResponseHeader>
0056    <BatchItem>
0057      <Operation type="Enumeration" value="Register"/>
0058      <ResultStatus type="Enumeration" value="Success"/>
0059      <ResponsePayload>
0060        <UniqueIdentifier type="TextString"
    value="$UNIQUE_IDENTIFIER_0"/>
```

```
0061        </ResponsePayload>
0062      </BatchItem>
0063    </ResponseMessage>
        # TIME 1
0064    <RequestMessage>
0065      <RequestHeader>
0066        <ProtocolVersion>
0067          <ProtocolVersionMajor type="Integer" value="1"/>
0068          <ProtocolVersionMinor type="Integer" value="2"/>
0069        </ProtocolVersion>
0070        <BatchCount type="Integer" value="1"/>
0071      </RequestHeader>
0072      <BatchItem>
0073        <Operation type="Enumeration" value="Encrypt"/>
0074        <RequestPayload>
0075          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0076          <Data type="ByteString"
          value="0102030405060708091011121314151601020304050607080910111213141
          51601"/>
0077          <IVCounterNonce type="ByteString"
          value="FF020304050607080910111213141516"/>
0078        </RequestPayload>
0079      </BatchItem>
0080    </RequestMessage>
0081    <ResponseMessage>
0082      <ResponseHeader>
0083        <ProtocolVersion>
0084          <ProtocolVersionMajor type="Integer" value="1"/>
0085          <ProtocolVersionMinor type="Integer" value="2"/>
0086        </ProtocolVersion>
0087        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0088        <BatchCount type="Integer" value="1"/>
0089      </ResponseHeader>
0090      <BatchItem>
0091        <Operation type="Enumeration" value="Encrypt"/>
0092        <ResultStatus type="Enumeration" value="Success"/>
0093        <ResponsePayload>
0094          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0095          <Data type="ByteString"
          value="e768203ba72b6e157daaad34b1e791d8e88457dc147942f01bfaff7b28a3c
          dde2203d4d5a4c7928ba9e9cc78b66a6546"/>
0096        </ResponsePayload>
0097      </BatchItem>
0098    </ResponseMessage>
        # TIME 2
        # Decrypt without the IV being specified will result in an error.
0099    <RequestMessage>
0100      <RequestHeader>
0101        <ProtocolVersion>
0102          <ProtocolVersionMajor type="Integer" value="1"/>
0103          <ProtocolVersionMinor type="Integer" value="2"/>
0104        </ProtocolVersion>
0105        <BatchCount type="Integer" value="1"/>
0106      </RequestHeader>
0107      <BatchItem>
0108        <Operation type="Enumeration" value="Decrypt"/>
```

```
0109      <RequestPayload>
0110        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0111        <Data type="ByteString"
          value="e768203ba72b6e157daaad34b1e791d8e88457dc147942f01bfaff7b28a3c
          dde2203d4d5a4c7928ba9e9cc78b66a6546"/>
0112      </RequestPayload>
0113    </BatchItem>
0114  </RequestMessage>
0115  <ResponseMessage>
0116    <ResponseHeader>
0117      <ProtocolVersion>
0118        <ProtocolVersionMajor type="Integer" value="1"/>
0119        <ProtocolVersionMinor type="Integer" value="2"/>
0120      </ProtocolVersion>
0121      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0122      <BatchCount type="Integer" value="1"/>
0123    </ResponseHeader>
0124    <BatchItem>
0125      <Operation type="Enumeration" value="Decrypt"/>
0126      <ResultStatus type="Enumeration" value="OperationFailed"/>
0127      <ResultReason type="Enumeration" value="InvalidMessage"/>
0128      <ResultMessage type="TextString" value="missing-iv"/>
0129    </BatchItem>
0130  </ResponseMessage>
          # TIME 3
          # Decrypt with the IV being specified
0131  <RequestMessage>
0132    <RequestHeader>
0133      <ProtocolVersion>
0134        <ProtocolVersionMajor type="Integer" value="1"/>
0135        <ProtocolVersionMinor type="Integer" value="2"/>
0136      </ProtocolVersion>
0137      <BatchCount type="Integer" value="1"/>
0138    </RequestHeader>
0139    <BatchItem>
0140      <Operation type="Enumeration" value="Decrypt"/>
0141      <RequestPayload>
0142        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0143        <Data type="ByteString"
          value="e768203ba72b6e157daaad34b1e791d8e88457dc147942f01bfaff7b28a3c
          dde2203d4d5a4c7928ba9e9cc78b66a6546"/>
0144        <IVCounterNonce type="ByteString"
          value="FF020304050607080910111213141516"/>
0145      </RequestPayload>
0146    </BatchItem>
0147  </RequestMessage>
0148  <ResponseMessage>
0149    <ResponseHeader>
0150      <ProtocolVersion>
0151        <ProtocolVersionMajor type="Integer" value="1"/>
0152        <ProtocolVersionMinor type="Integer" value="2"/>
0153      </ProtocolVersion>
0154      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0155      <BatchCount type="Integer" value="1"/>
0156    </ResponseHeader>
0157    <BatchItem>
```

```
0158      <Operation type="Enumeration" value="Decrypt"/>
0159      <ResultStatus type="Enumeration" value="Success"/>
0160      <ResponsePayload>
0161        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0162        <Data type="ByteString"
          value="0102030405060708091011121314151601020304050607080910111213141
          51601"/>
0163      </ResponsePayload>
0164    </BatchItem>
0165  </ResponseMessage>
      # TIME 4
0166  <RequestMessage>
0167    <RequestHeader>
0168      <ProtocolVersion>
0169        <ProtocolVersionMajor type="Integer" value="1"/>
0170        <ProtocolVersionMinor type="Integer" value="2"/>
0171      </ProtocolVersion>
0172      <BatchCount type="Integer" value="1"/>
0173    </RequestHeader>
0174    <BatchItem>
0175      <Operation type="Enumeration" value="Revoke"/>
0176      <RequestPayload>
0177        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0178        <RevocationReason>
0179          <RevocationReasonCode type="Enumeration"
          value="Unspecified"/>
0180        </RevocationReason>
0181      </RequestPayload>
0182    </BatchItem>
0183  </RequestMessage>
0184  <ResponseMessage>
0185    <ResponseHeader>
0186      <ProtocolVersion>
0187        <ProtocolVersionMajor type="Integer" value="1"/>
0188        <ProtocolVersionMinor type="Integer" value="2"/>
0189      </ProtocolVersion>
0190      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0191      <BatchCount type="Integer" value="1"/>
0192    </ResponseHeader>
0193    <BatchItem>
0194      <Operation type="Enumeration" value="Revoke"/>
0195      <ResultStatus type="Enumeration" value="Success"/>
0196      <ResponsePayload>
0197        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0198      </ResponsePayload>
0199    </BatchItem>
0200  </ResponseMessage>
      # TIME 5
0201  <RequestMessage>
0202    <RequestHeader>
0203      <ProtocolVersion>
0204        <ProtocolVersionMajor type="Integer" value="1"/>
0205        <ProtocolVersionMinor type="Integer" value="2"/>
0206      </ProtocolVersion>
0207      <BatchCount type="Integer" value="1"/>
```

```
0208    </RequestHeader>
0209    <BatchItem>
0210      <Operation type="Enumeration" value="Destroy"/>
0211      <RequestPayload>
0212        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0213      </RequestPayload>
0214    </BatchItem>
0215  </RequestMessage>
```

```
0216  <ResponseMessage>
0217    <ResponseHeader>
0218      <ProtocolVersion>
0219        <ProtocolVersionMajor type="Integer" value="1"/>
0220        <ProtocolVersionMinor type="Integer" value="2"/>
0221      </ProtocolVersion>
0222      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0223      <BatchCount type="Integer" value="1"/>
0224    </ResponseHeader>
0225    <BatchItem>
0226      <Operation type="Enumeration" value="Destroy"/>
0227      <ResultStatus type="Enumeration" value="Success"/>
0228      <ResponsePayload>
0229        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0230      </ResponsePayload>
0231    </BatchItem>
0232  </ResponseMessage>
```

166

167 3.1.13 CS-BC-M-13-12 - Encrypt and Decrypt with Known Symmetric Key
168 and PKCS5 Padding and CBC and Random IV

169 Register a symmetric key and perform encrypt using the symmetric key followed by decrypt. The input
170 data is non-block size. The Cryptographic Parameters are associated attributes of the key rather than
171 parameters to the operation. This is otherwise the same as CS-BC-M-12-12.

```
      # TIME 0
0001  <RequestMessage>
0002    <RequestHeader>
0003      <ProtocolVersion>
0004        <ProtocolVersionMajor type="Integer" value="1"/>
0005        <ProtocolVersionMinor type="Integer" value="2"/>
0006      </ProtocolVersion>
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="Register"/>
0011      <RequestPayload>
0012        <ObjectType type="Enumeration" value="SymmetricKey"/>
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
        Usage Mask"/>
0016            <AttributeValue type="Integer" value="Encrypt Decrypt"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="x-ID"/>
0020            <AttributeValue type="TextString" value="CS-BC-M-13-12"/>
```

```
0021          </Attribute>
0022          <Attribute>
0023            <AttributeName type="TextString" value="Activation Date"/>
0024            <AttributeValue type="DateTime" value="$NOW-3600"/>
0025          </Attribute>
0026          <Attribute>
0027            <AttributeName type="TextString" value="Cryptographic
      Parameters"/>
0028          <AttributeValue>
0029            <BlockCipherMode type="Enumeration" value="CBC"/>
0030            <PaddingMethod type="Enumeration" value="PKCS5"/>
0031            <RandomIV type="Boolean" value="true"/>
0032          </AttributeValue>
0033          </Attribute>
0034        </TemplateAttribute>
0035        <SymmetricKey>
0036          <KeyBlock>
0037            <KeyFormatType type="Enumeration" value="Raw"/>
0038            <KeyValue>
0039              <KeyMaterial type="ByteString"
      value="0123456789abcdef0123456789abcdef"/>
0040            </KeyValue>
0041            <CryptographicAlgorithm type="Enumeration" value="AES"/>
0042            <CryptographicLength type="Integer" value="128"/>
0043          </KeyBlock>
0044        </SymmetricKey>
0045      </RequestPayload>
0046    </BatchItem>
0047  </RequestMessage>
```

```
0048  <ResponseMessage>
0049    <ResponseHeader>
0050      <ProtocolVersion>
0051        <ProtocolVersionMajor type="Integer" value="1"/>
0052        <ProtocolVersionMinor type="Integer" value="2"/>
0053      </ProtocolVersion>
0054      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0055      <BatchCount type="Integer" value="1"/>
0056    </ResponseHeader>
0057    <BatchItem>
0058      <Operation type="Enumeration" value="Register"/>
0059      <ResultStatus type="Enumeration" value="Success"/>
0060      <ResponsePayload>
0061        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0062      </ResponsePayload>
0063    </BatchItem>
0064  </ResponseMessage>
```

```
      # TIME 1
0065  <RequestMessage>
0066    <RequestHeader>
0067      <ProtocolVersion>
0068        <ProtocolVersionMajor type="Integer" value="1"/>
0069        <ProtocolVersionMinor type="Integer" value="2"/>
0070      </ProtocolVersion>
0071      <BatchCount type="Integer" value="1"/>
0072    </RequestHeader>
0073    <BatchItem>
0074      <Operation type="Enumeration" value="Encrypt"/>
```

```
0075      <RequestPayload>
0076        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0077        <Data type="ByteString"
          value="0102030405060708091011121314151601020304050607080910111213141
          51601"/>
0078      </RequestPayload>
0079    </BatchItem>
0080  </RequestMessage>
0081  <ResponseMessage>
0082    <ResponseHeader>
0083      <ProtocolVersion>
0084        <ProtocolVersionMajor type="Integer" value="1"/>
0085        <ProtocolVersionMinor type="Integer" value="2"/>
0086      </ProtocolVersion>
0087      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0088      <BatchCount type="Integer" value="1"/>
0089    </ResponseHeader>
0090    <BatchItem>
0091      <Operation type="Enumeration" value="Encrypt"/>
0092      <ResultStatus type="Enumeration" value="Success"/>
0093      <ResponsePayload>
0094        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0095        <Data type="ByteString"
          value="e768203ba72b6e157daaad34b1e791d8e88457dc147942f01bfaff7b28a3c
          dde2203d4d5a4c7928ba9e9cc78b66a6546"/>
0096        <IVCounterNonce type="ByteString"
          value="FF020304050607080910111213141516"/>
0097      </ResponsePayload>
0098    </BatchItem>
0099  </ResponseMessage>
          # TIME 2
          # Decrypt without the IV being specified will result in an error.
0100  <RequestMessage>
0101    <RequestHeader>
0102      <ProtocolVersion>
0103        <ProtocolVersionMajor type="Integer" value="1"/>
0104        <ProtocolVersionMinor type="Integer" value="2"/>
0105      </ProtocolVersion>
0106      <BatchCount type="Integer" value="1"/>
0107    </RequestHeader>
0108    <BatchItem>
0109      <Operation type="Enumeration" value="Decrypt"/>
0110      <RequestPayload>
0111        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0112        <Data type="ByteString" value="$DATA_0"/>
0113      </RequestPayload>
0114    </BatchItem>
0115  </RequestMessage>
0116  <ResponseMessage>
0117    <ResponseHeader>
0118      <ProtocolVersion>
0119        <ProtocolVersionMajor type="Integer" value="1"/>
0120        <ProtocolVersionMinor type="Integer" value="2"/>
0121      </ProtocolVersion>
0122      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
```

```
0123      <BatchCount type="Integer" value="1"/>
0124    </ResponseHeader>
0125    <BatchItem>
0126      <Operation type="Enumeration" value="Decrypt"/>
0127      <ResultStatus type="Enumeration" value="OperationFailed"/>
0128      <ResultReason type="Enumeration" value="InvalidMessage"/>
0129      <ResultMessage type="TextString" value="missing-iv"/>
0130    </BatchItem>
0131  </ResponseMessage>
```

```
      # TIME 3
      # Decrypt with the IV being specified
0132  <RequestMessage>
0133    <RequestHeader>
0134      <ProtocolVersion>
0135        <ProtocolVersionMajor type="Integer" value="1"/>
0136        <ProtocolVersionMinor type="Integer" value="2"/>
0137      </ProtocolVersion>
0138      <BatchCount type="Integer" value="1"/>
0139    </RequestHeader>
0140    <BatchItem>
0141      <Operation type="Enumeration" value="Decrypt"/>
0142      <RequestPayload>
0143        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0144        <Data type="ByteString" value="$DATA_0"/>
0145        <IVCounterNonce type="ByteString" value="$IV_COUNTER_NONCE"/>
0146      </RequestPayload>
0147    </BatchItem>
0148  </RequestMessage>
```

```
0149  <ResponseMessage>
0150    <ResponseHeader>
0151      <ProtocolVersion>
0152        <ProtocolVersionMajor type="Integer" value="1"/>
0153        <ProtocolVersionMinor type="Integer" value="2"/>
0154      </ProtocolVersion>
0155      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0156      <BatchCount type="Integer" value="1"/>
0157    </ResponseHeader>
0158    <BatchItem>
0159      <Operation type="Enumeration" value="Decrypt"/>
0160      <ResultStatus type="Enumeration" value="Success"/>
0161      <ResponsePayload>
0162        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0163        <Data type="ByteString"
      value="0102030405060708091011121314151601020304050607080910111213141
      51601"/>
0164      </ResponsePayload>
0165    </BatchItem>
0166  </ResponseMessage>
```

```
      # TIME 4
0167  <RequestMessage>
0168    <RequestHeader>
0169      <ProtocolVersion>
0170        <ProtocolVersionMajor type="Integer" value="1"/>
0171        <ProtocolVersionMinor type="Integer" value="2"/>
0172      </ProtocolVersion>
0173      <BatchCount type="Integer" value="1"/>
```

```
0174    </RequestHeader>
0175    <BatchItem>
0176      <Operation type="Enumeration" value="Revoke"/>
0177      <RequestPayload>
0178        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0179        <RevocationReason>
0180          <RevocationReasonCode type="Enumeration"
        value="Unspecified"/>
0181        </RevocationReason>
0182      </RequestPayload>
0183    </BatchItem>
0184  </RequestMessage>
0185  <ResponseMessage>
0186    <ResponseHeader>
0187      <ProtocolVersion>
0188        <ProtocolVersionMajor type="Integer" value="1"/>
0189        <ProtocolVersionMinor type="Integer" value="2"/>
0190      </ProtocolVersion>
0191      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0192      <BatchCount type="Integer" value="1"/>
0193    </ResponseHeader>
0194    <BatchItem>
0195      <Operation type="Enumeration" value="Revoke"/>
0196      <ResultStatus type="Enumeration" value="Success"/>
0197      <ResponsePayload>
0198        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0199      </ResponsePayload>
0200    </BatchItem>
0201  </ResponseMessage>
        # TIME 5
0202  <RequestMessage>
0203    <RequestHeader>
0204      <ProtocolVersion>
0205        <ProtocolVersionMajor type="Integer" value="1"/>
0206        <ProtocolVersionMinor type="Integer" value="2"/>
0207      </ProtocolVersion>
0208      <BatchCount type="Integer" value="1"/>
0209    </RequestHeader>
0210    <BatchItem>
0211      <Operation type="Enumeration" value="Destroy"/>
0212      <RequestPayload>
0213        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0214      </RequestPayload>
0215    </BatchItem>
0216  </RequestMessage>
0217  <ResponseMessage>
0218    <ResponseHeader>
0219      <ProtocolVersion>
0220        <ProtocolVersionMajor type="Integer" value="1"/>
0221        <ProtocolVersionMinor type="Integer" value="2"/>
0222      </ProtocolVersion>
0223      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0224      <BatchCount type="Integer" value="1"/>
0225    </ResponseHeader>
0226    <BatchItem>
```

```
0227      <Operation type="Enumeration" value="Destroy"/>
0228      <ResultStatus type="Enumeration" value="Success"/>
0229      <ResponsePayload>
0230        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0231      </ResponsePayload>
0232    </BatchItem>
0233  </ResponseMessage>
```

172

173 3.1.14 CS-BC-M-14-12 - Encrypt and Decrypt with Known Symmetric Key
174 Date Checks

175 Register a symmetric key and perform both encrypt and decrypt operations using the symmetric key
176 outside of the valid Process Start Date and Protect Stop Date to confirm the operations fail.

177 The Process Start Date is set to a future date. The Protect Stop Date is set to a past date.

178 This is a modified version of CS-BC-M-6-12.

```
      # TIME 0
0001  <RequestMessage>
0002    <RequestHeader>
0003      <ProtocolVersion>
0004        <ProtocolVersionMajor type="Integer" value="1"/>
0005        <ProtocolVersionMinor type="Integer" value="2"/>
0006      </ProtocolVersion>
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="Register"/>
0011      <RequestPayload>
0012        <ObjectType type="Enumeration" value="SymmetricKey"/>
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
      Usage Mask"/>
0016            <AttributeValue type="Integer" value="Encrypt Decrypt"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="x-ID"/>
0020            <AttributeValue type="TextString" value="CS-BC-M-14-12"/>
0021          </Attribute>
0022          <Attribute>
0023            <AttributeName type="TextString" value="Activation Date"/>
0024            <AttributeValue type="DateTime" value="$NOW-3600"/>
0025          </Attribute>
0026          <Attribute>
0027            <AttributeName type="TextString" value="Process Start
      Date"/>
0028            <AttributeValue type="DateTime" value="$NOW+3600"/>
0029          </Attribute>
0030          <Attribute>
0031            <AttributeName type="TextString" value="Protect Stop
      Date"/>
0032            <AttributeValue type="DateTime" value="$NOW-3600"/>
0033          </Attribute>
0034        </TemplateAttribute>
0035        <SymmetricKey>
```

```
0036          <KeyBlock>
0037            <KeyFormatType type="Enumeration" value="Raw"/>
0038            <KeyValue>
0039              <KeyMaterial type="ByteString"
      value="0123456789abcdef0123456789abcdef"/>
0040            </KeyValue>
0041            <CryptographicAlgorithm type="Enumeration" value="AES"/>
0042            <CryptographicLength type="Integer" value="128"/>
0043          </KeyBlock>
0044        </SymmetricKey>
0045      </RequestPayload>
0046    </BatchItem>
0047  </RequestMessage>
```

```
0048  <ResponseMessage>
0049    <ResponseHeader>
0050      <ProtocolVersion>
0051        <ProtocolVersionMajor type="Integer" value="1"/>
0052        <ProtocolVersionMinor type="Integer" value="2"/>
0053      </ProtocolVersion>
0054      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0055      <BatchCount type="Integer" value="1"/>
0056    </ResponseHeader>
0057    <BatchItem>
0058      <Operation type="Enumeration" value="Register"/>
0059      <ResultStatus type="Enumeration" value="Success"/>
0060      <ResponsePayload>
0061        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0062      </ResponsePayload>
0063    </BatchItem>
0064  </ResponseMessage>
```

```
      # TIME 1
0065  <RequestMessage>
0066    <RequestHeader>
0067      <ProtocolVersion>
0068        <ProtocolVersionMajor type="Integer" value="1"/>
0069        <ProtocolVersionMinor type="Integer" value="2"/>
0070      </ProtocolVersion>
0071      <BatchCount type="Integer" value="1"/>
0072    </RequestHeader>
0073    <BatchItem>
0074      <Operation type="Enumeration" value="Encrypt"/>
0075      <RequestPayload>
0076        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0077        <CryptographicParameters>
0078        <BlockCipherMode type="Enumeration" value="ECB"/>
0079        </CryptographicParameters>
0080        <Data type="ByteString"
      value="0102030405060708091011121314151 6"/>
0081      </RequestPayload>
0082    </BatchItem>
0083  </RequestMessage>
```

```
0084  <ResponseMessage>
0085    <ResponseHeader>
0086      <ProtocolVersion>
0087        <ProtocolVersionMajor type="Integer" value="1"/>
0088        <ProtocolVersionMinor type="Integer" value="2"/>
```

```
0089      </ProtocolVersion>
0090      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0091      <BatchCount type="Integer" value="1"/>
0092    </ResponseHeader>
0093    <BatchItem>
0094      <Operation type="Enumeration" value="Encrypt"/>
0095      <ResultStatus type="Enumeration" value="OperationFailed"/>
0096      <ResultReason type="Enumeration" value="PermissionDenied"/>
0097      <ResultMessage type="TextString" value="DENIED"/>
0098    </BatchItem>
0099  </ResponseMessage>
```

```
      # TIME 2
0100  <RequestMessage>
0101    <RequestHeader>
0102      <ProtocolVersion>
0103        <ProtocolVersionMajor type="Integer" value="1"/>
0104        <ProtocolVersionMinor type="Integer" value="2"/>
0105      </ProtocolVersion>
0106      <BatchCount type="Integer" value="1"/>
0107    </RequestHeader>
0108    <BatchItem>
0109      <Operation type="Enumeration" value="Decrypt"/>
0110      <RequestPayload>
0111        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0112        <CryptographicParameters>
0113        <BlockCipherMode type="Enumeration" value="ECB"/>
0114        </CryptographicParameters>
0115        <Data type="ByteString"
      value="fd912d102dbb482f6f6e91bd57119095"/>
0116      </RequestPayload>
0117    </BatchItem>
0118  </RequestMessage>
```

```
0119  <ResponseMessage>
0120    <ResponseHeader>
0121      <ProtocolVersion>
0122        <ProtocolVersionMajor type="Integer" value="1"/>
0123        <ProtocolVersionMinor type="Integer" value="2"/>
0124      </ProtocolVersion>
0125      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0126      <BatchCount type="Integer" value="1"/>
0127    </ResponseHeader>
0128    <BatchItem>
0129      <Operation type="Enumeration" value="Decrypt"/>
0130      <ResultStatus type="Enumeration" value="OperationFailed"/>
0131      <ResultReason type="Enumeration" value="PermissionDenied"/>
0132      <ResultMessage type="TextString" value="DENIED"/>
0133    </BatchItem>
0134  </ResponseMessage>
```

```
      # TIME 3
0135  <RequestMessage>
0136    <RequestHeader>
0137      <ProtocolVersion>
0138        <ProtocolVersionMajor type="Integer" value="1"/>
0139        <ProtocolVersionMinor type="Integer" value="2"/>
0140      </ProtocolVersion>
0141      <BatchCount type="Integer" value="1"/>
0142    </RequestHeader>
```

```
0143    <BatchItem>
0144      <Operation type="Enumeration" value="Revoke"/>
0145      <RequestPayload>
0146        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0147        <RevocationReason>
0148          <RevocationReasonCode type="Enumeration"
        value="Unspecified"/>
0149        </RevocationReason>
0150      </RequestPayload>
0151    </BatchItem>
0152  </RequestMessage>
0153  <ResponseMessage>
0154    <ResponseHeader>
0155      <ProtocolVersion>
0156        <ProtocolVersionMajor type="Integer" value="1"/>
0157        <ProtocolVersionMinor type="Integer" value="2"/>
0158      </ProtocolVersion>
0159      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0160      <BatchCount type="Integer" value="1"/>
0161    </ResponseHeader>
0162    <BatchItem>
0163      <Operation type="Enumeration" value="Revoke"/>
0164      <ResultStatus type="Enumeration" value="Success"/>
0165      <ResponsePayload>
0166        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0167      </ResponsePayload>
0168    </BatchItem>
0169  </ResponseMessage>
        # TIME 4
0170  <RequestMessage>
0171    <RequestHeader>
0172      <ProtocolVersion>
0173        <ProtocolVersionMajor type="Integer" value="1"/>
0174        <ProtocolVersionMinor type="Integer" value="2"/>
0175      </ProtocolVersion>
0176      <BatchCount type="Integer" value="1"/>
0177    </RequestHeader>
0178    <BatchItem>
0179      <Operation type="Enumeration" value="Destroy"/>
0180      <RequestPayload>
0181        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0182      </RequestPayload>
0183    </BatchItem>
0184  </RequestMessage>
0185  <ResponseMessage>
0186    <ResponseHeader>
0187      <ProtocolVersion>
0188        <ProtocolVersionMajor type="Integer" value="1"/>
0189        <ProtocolVersionMinor type="Integer" value="2"/>
0190      </ProtocolVersion>
0191      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0192      <BatchCount type="Integer" value="1"/>
0193    </ResponseHeader>
0194    <BatchItem>
0195      <Operation type="Enumeration" value="Destroy"/>
```

```
0196      <ResultStatus type="Enumeration" value="Success"/>
0197      <ResponsePayload>
0198        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0199      </ResponsePayload>
0200    </BatchItem>
0201  </ResponseMessage>
```

179

180 3.2 Mandatory Test Cases KMIP v1.2 - Advanced

181 3.2.1 CS-AC-M-1-12 - Sign with Known Asymmetric Key

182 Register an asymmetric key and perform sign using the asymmetric key.

```
      # TIME 0
0001  <RequestMessage>
0002    <RequestHeader>
0003      <ProtocolVersion>
0004        <ProtocolVersionMajor type="Integer" value="1"/>
0005        <ProtocolVersionMinor type="Integer" value="2"/>
0006      </ProtocolVersion>
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="Register"/>
0011      <RequestPayload>
0012        <ObjectType type="Enumeration" value="PrivateKey"/>
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
          Usage Mask"/>
0016            <AttributeValue type="Integer" value="Sign"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="Cryptographic
          Parameters"/>
0020            <AttributeValue>
0021              <PaddingMethod type="Enumeration" value="PSS"/>
0022              <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0023              <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0024            </AttributeValue>
0025          </Attribute>
0026          <Attribute>
0027            <AttributeName type="TextString" value="x-ID"/>
0028            <AttributeValue type="TextString" value="CS-AC-M-1-12-
          prikey1"/>
0029          </Attribute>
0030          <Attribute>
0031            <AttributeName type="TextString" value="Activation Date"/>
0032            <AttributeValue type="DateTime" value="$NOW-3600"/>
0033          </Attribute>
0034        </TemplateAttribute>
0035        <PrivateKey>
0036          <KeyBlock>
0037            <KeyFormatType type="Enumeration" value="PKCS_1"/>
0038            <KeyValue>
0039              <KeyMaterial type="ByteString"
```

```
      value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353
      57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483
      46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa
      2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650
      89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c
      795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f
      91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281
      5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050
      203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a
      7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f
      a74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b
      2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0
      e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a
      a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e
      3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78
      965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8
      c3cdc2464744a793713dafb9f1dbc799ff96423fecd3cba794286bce920f4b5c183f
      99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967
      4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c
      ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064
      b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e
      59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4
      990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766
      b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab
      7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0
      e94ad1ee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db
      e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa
      e1ebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2
      7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eaefa922fd75d5b16b1a5
      61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bff1a85a72
      6a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171
      666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520
      a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a
      1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d34941
      7e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f812
      9c32341a8b44f"/>
0040            </KeyValue>
0041            <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0042            <CryptographicLength type="Integer" value="2048"/>
0043          </KeyBlock>
0044        </PrivateKey>
0045      </RequestPayload>
0046    </BatchItem>
0047  </RequestMessage>
0048  <ResponseMessage>
0049    <ResponseHeader>
0050      <ProtocolVersion>
0051        <ProtocolVersionMajor type="Integer" value="1"/>
0052        <ProtocolVersionMinor type="Integer" value="2"/>
0053      </ProtocolVersion>
0054      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0055      <BatchCount type="Integer" value="1"/>
0056    </ResponseHeader>
0057    <BatchItem>
0058      <Operation type="Enumeration" value="Register"/>
0059      <ResultStatus type="Enumeration" value="Success"/>
0060      <ResponsePayload>
0061        <UniqueIdentifier type="TextString"
```

```
value="$UNIQUE_IDENTIFIER_0"/>
    </ResponsePayload>
  </BatchItem>
</ResponseMessage>
```

```
# TIME 1
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Sign"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
      <Data type="ByteString"
value="0102030405060708091011121314151 6"/>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Sign"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
      <SignatureData type="ByteString"
value="9d888ed8c169ebc052e21f7392427b0efa78321f64558ac4dba2277f0b22c
3a94eb098a608ef2a70931eece25482e5c962a560fe73f83471779a69d85099ff44f
e5da16977fe9f92bdd26a153612d57f325c619570577f81eff22ca511c684bc037a5
79981c899c91da6d1ac34c230fa68db59c3f31bc5add7c75328f9974f342f1bb5e92
8b89619894fb301002ef60a1d093dfc22f87c442c13cb8a6cd83be0ecc5b18647c51
fb92238a90fbd3e4aaf37612ab4b76243bda44db4a48a88b0899fa672d06f7b4c109
4858e7257c4851447ca29dbbc11a664c0cd8be7ce7b27173fa8042d54d240ade8ee6
069459ec08bf510eaf68e2fc1e50561dc686525ba0f"/>
    </ResponsePayload>
  </BatchItem>
</ResponseMessage>
```

```
# TIME 2
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
```

```
0106    </RequestHeader>
0107    <BatchItem>
0108      <Operation type="Enumeration" value="Revoke"/>
0109      <RequestPayload>
0110        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0111        <RevocationReason>
0112          <RevocationReasonCode type="Enumeration"
        value="Unspecified"/>
0113        </RevocationReason>
0114      </RequestPayload>
0115    </BatchItem>
0116  </RequestMessage>
0117  <ResponseMessage>
0118    <ResponseHeader>
0119      <ProtocolVersion>
0120        <ProtocolVersionMajor type="Integer" value="1"/>
0121        <ProtocolVersionMinor type="Integer" value="2"/>
0122      </ProtocolVersion>
0123      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0124      <BatchCount type="Integer" value="1"/>
0125    </ResponseHeader>
0126    <BatchItem>
0127      <Operation type="Enumeration" value="Revoke"/>
0128      <ResultStatus type="Enumeration" value="Success"/>
0129      <ResponsePayload>
0130        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0131      </ResponsePayload>
0132    </BatchItem>
0133  </ResponseMessage>
        # TIME 3
0134  <RequestMessage>
0135    <RequestHeader>
0136      <ProtocolVersion>
0137        <ProtocolVersionMajor type="Integer" value="1"/>
0138        <ProtocolVersionMinor type="Integer" value="2"/>
0139      </ProtocolVersion>
0140      <BatchCount type="Integer" value="1"/>
0141    </RequestHeader>
0142    <BatchItem>
0143      <Operation type="Enumeration" value="Destroy"/>
0144      <RequestPayload>
0145        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0146      </RequestPayload>
0147    </BatchItem>
0148  </RequestMessage>
0149  <ResponseMessage>
0150    <ResponseHeader>
0151      <ProtocolVersion>
0152        <ProtocolVersionMajor type="Integer" value="1"/>
0153        <ProtocolVersionMinor type="Integer" value="2"/>
0154      </ProtocolVersion>
0155      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0156      <BatchCount type="Integer" value="1"/>
0157    </ResponseHeader>
0158    <BatchItem>
```

```
0159      <Operation type="Enumeration" value="Destroy"/>
0160      <ResultStatus type="Enumeration" value="Success"/>
0161      <ResponsePayload>
0162        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0163      </ResponsePayload>
0164    </BatchItem>
0165  </ResponseMessage>
```

183

184 3.2.2 CS-AC-M-2-12 - Signature Verify with Known Asymmetric Key

185 Register an asymmetric key and perform signature verify using the asymmetric key.

```
      # TIME 0
0001  <RequestMessage>
0002    <RequestHeader>
0003      <ProtocolVersion>
0004        <ProtocolVersionMajor type="Integer" value="1"/>
0005        <ProtocolVersionMinor type="Integer" value="2"/>
0006      </ProtocolVersion>
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="Register"/>
0011      <RequestPayload>
0012        <ObjectType type="Enumeration" value="PublicKey"/>
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
      Usage Mask"/>
0016            <AttributeValue type="Integer" value="Verify"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="x-ID"/>
0020            <AttributeValue type="TextString" value="CS-AC-M-2-12-
      pubkey1"/>
0021          </Attribute>
0022          <Attribute>
0023            <AttributeName type="TextString" value="Activation Date"/>
0024            <AttributeValue type="DateTime" value="$NOW-3600"/>
0025          </Attribute>
0026          <Attribute>
0027            <AttributeName type="TextString" value="Cryptographic
      Parameters"/>
0028            <AttributeValue>
0029              <PaddingMethod type="Enumeration" value="PSS"/>
0030              <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0031              <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0032            </AttributeValue>
0033          </Attribute>
0034        </TemplateAttribute>
0035        <PublicKey>
0036          <KeyBlock>
0037            <KeyFormatType type="Enumeration" value="PKCS_1"/>
0038            <KeyValue>
0039              <KeyMaterial type="ByteString"
      value="3082010a0282010100ab7f161c0042496ccd6c6d4dadb9199734353577760
```

```
03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b
8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89
b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981
35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328
abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013
da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612
a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010
001"/>
0040            </KeyValue>
0041            <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0042            <CryptographicLength type="Integer" value="2048"/>
0043          </KeyBlock>
0044        </PublicKey>
0045      </RequestPayload>
0046    </BatchItem>
0047  </RequestMessage>
0048  <ResponseMessage>
0049    <ResponseHeader>
0050      <ProtocolVersion>
0051        <ProtocolVersionMajor type="Integer" value="1"/>
0052        <ProtocolVersionMinor type="Integer" value="2"/>
0053      </ProtocolVersion>
0054      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0055      <BatchCount type="Integer" value="1"/>
0056    </ResponseHeader>
0057    <BatchItem>
0058      <Operation type="Enumeration" value="Register"/>
0059      <ResultStatus type="Enumeration" value="Success"/>
0060      <ResponsePayload>
0061        <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0062      </ResponsePayload>
0063    </BatchItem>
0064  </ResponseMessage>
  # TIME 1
0065  <RequestMessage>
0066    <RequestHeader>
0067      <ProtocolVersion>
0068        <ProtocolVersionMajor type="Integer" value="1"/>
0069        <ProtocolVersionMinor type="Integer" value="2"/>
0070      </ProtocolVersion>
0071      <BatchCount type="Integer" value="1"/>
0072    </RequestHeader>
0073    <BatchItem>
0074      <Operation type="Enumeration" value="SignatureVerify"/>
0075      <RequestPayload>
0076        <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0077        <Data type="ByteString"
value="0102030405060708091011121314151 6"/>
0078        <SignatureData type="ByteString"
value="2925ebf8c6c9d0585c36a44491dd28f8ffd1098d2275a505a0eba7af452e9
496472fd5c4a515d1c0db16c7c59ef76863b571cbf498fb8178ffeb75667e6e51b9b
9bbf09d55bba54b42acb947aa5a81dc62751727d7cad4616c0c0bf1dd666f8266f24
262c5fa9cbbdc424ef5f5e345e633d111e66eb4afc4001bb02e158b2d5d4573c6146
55f21a688bee0e9dbde6a58324c08f42ae69697e0c51803f9de6b3df242d2915d9b1
a8110ad28143ab7855ef92ede48971b484172de3b0b8957f493a74b3372ee2200f22
33607735f90d0b180968ab20d74841fd3dba4fb1f225ea5c6c87f99c2a238db72a53
```

```
        6e68be202a092cd032337d451477e568f9a48b638cb"/>
0079        </RequestPayload>
0080      </BatchItem>
0081    </RequestMessage>
0082    <ResponseMessage>
0083      <ResponseHeader>
0084        <ProtocolVersion>
0085          <ProtocolVersionMajor type="Integer" value="1"/>
0086          <ProtocolVersionMinor type="Integer" value="2"/>
0087        </ProtocolVersion>
0088        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0089        <BatchCount type="Integer" value="1"/>
0090      </ResponseHeader>
0091      <BatchItem>
0092        <Operation type="Enumeration" value="SignatureVerify"/>
0093        <ResultStatus type="Enumeration" value="Success"/>
0094        <ResponsePayload>
0095          <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0096          <ValidityIndicator type="Enumeration" value="Valid"/>
0097        </ResponsePayload>
0098      </BatchItem>
0099    </ResponseMessage>
        # TIME 2
        # Check that an invalid data input fails to match the signature
0100    <RequestMessage>
0101      <RequestHeader>
0102        <ProtocolVersion>
0103          <ProtocolVersionMajor type="Integer" value="1"/>
0104          <ProtocolVersionMinor type="Integer" value="2"/>
0105        </ProtocolVersion>
0106        <BatchCount type="Integer" value="1"/>
0107      </RequestHeader>
0108      <BatchItem>
0109        <Operation type="Enumeration" value="SignatureVerify"/>
0110        <RequestPayload>
0111          <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0112          <Data type="ByteString"
        value="FF020304050607080910111213141516"/>
0113          <SignatureData type="ByteString"
        value="2925ebf8c6c9d0585c36a44491dd28f8ffd1098d2275a505a0eba7af452e9
        496472fd5c4a515d1c0db16c7c59ef76863b571cbf498fb8178ffeb75667e6e51b9b
        9bbf09d55bba54b42acb947aa5a81dc62751727d7cad4616c0c0bf1dd666f8266f24
        262c5fa9cbbdc424ef5f5e345e633d111e66eb4afc4001bb02e158b2d5d4573c6146
        55f21a688bee0e9dbde6a58324c08f42ae69697e0c51803f9de6b3df242d2915d9b1
        a8110ad28143ab7855ef92ede48971b484172de3b0b8957f493a74b3372ee2200f22
        33607735f90d0b180968ab20d74841fd3dba4fb1f225ea5c6c87f99c2a238db72a53
        6e68be202a092cd032337d451477e568f9a48b638cb"/>
0114        </RequestPayload>
0115      </BatchItem>
0116    </RequestMessage>
0117    <ResponseMessage>
0118      <ResponseHeader>
0119        <ProtocolVersion>
0120          <ProtocolVersionMajor type="Integer" value="1"/>
0121          <ProtocolVersionMinor type="Integer" value="2"/>
0122        </ProtocolVersion>
```

```
0123        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0124        <BatchCount type="Integer" value="1"/>
0125      </ResponseHeader>
0126      <BatchItem>
0127        <Operation type="Enumeration" value="SignatureVerify"/>
0128        <ResultStatus type="Enumeration" value="Success"/>
0129        <ResponsePayload>
0130          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0131          <ValidityIndicator type="Enumeration" value="Invalid"/>
0132        </ResponsePayload>
0133      </BatchItem>
0134    </ResponseMessage>
```

```
          # TIME 3
          # Check that an invalid signature input fails to match the signature
0135    <RequestMessage>
0136      <RequestHeader>
0137        <ProtocolVersion>
0138          <ProtocolVersionMajor type="Integer" value="1"/>
0139          <ProtocolVersionMinor type="Integer" value="2"/>
0140        </ProtocolVersion>
0141        <BatchCount type="Integer" value="1"/>
0142      </RequestHeader>
0143      <BatchItem>
0144        <Operation type="Enumeration" value="SignatureVerify"/>
0145        <RequestPayload>
0146          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0147          <Data type="ByteString"
          value="0102030405060708091011121314151 6"/>
0148          <SignatureData type="ByteString"
          value="FF25ebf8c6c9d0585c36a44491dd28f8ffd1098d2275a505a0eba7af452e9
          496472fd5c4a515d1c0db16c7c59ef76863b571cbf498fb8178ffeb75667e6e51b9b
          9bbf09d55bba54b42acb947aa5a81dc62751727d7cad4616c0c0bf1dd666f8266f24
          262c5fa9cbbdc424ef5f5e345e633d111e66eb4afc4001bb02e158b2d5d4573c6146
          55f21a688bee0e9dbde6a58324c08f42ae69697e0c51803f9de6b3df242d2915d9b1
          a8110ad28143ab7855ef92ede48971b484172de3b0b8957f493a74b3372ee2200f22
          33607735f90d0b180968ab20d74841fd3dba4fb1f225ea5c6c87f99c2a238db72a53
          6e68be202a092cd032337d451477e568f9a48b638cb"/>
0149      </RequestPayload>
0150    </BatchItem>
0151  </RequestMessage>
```

```
0152  <ResponseMessage>
0153    <ResponseHeader>
0154      <ProtocolVersion>
0155        <ProtocolVersionMajor type="Integer" value="1"/>
0156        <ProtocolVersionMinor type="Integer" value="2"/>
0157      </ProtocolVersion>
0158      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0159      <BatchCount type="Integer" value="1"/>
0160    </ResponseHeader>
0161    <BatchItem>
0162      <Operation type="Enumeration" value="SignatureVerify"/>
0163      <ResultStatus type="Enumeration" value="Success"/>
0164      <ResponsePayload>
0165        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0166        <ValidityIndicator type="Enumeration" value="Invalid"/>
```

```
0167      </ResponsePayload>
0168    </BatchItem>
0169  </ResponseMessage>
```

```
      # TIME 4
0170  <RequestMessage>
0171    <RequestHeader>
0172      <ProtocolVersion>
0173        <ProtocolVersionMajor type="Integer" value="1"/>
0174        <ProtocolVersionMinor type="Integer" value="2"/>
0175      </ProtocolVersion>
0176      <BatchCount type="Integer" value="1"/>
0177    </RequestHeader>
0178    <BatchItem>
0179      <Operation type="Enumeration" value="Revoke"/>
0180      <RequestPayload>
0181        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0182        <RevocationReason>
0183          <RevocationReasonCode type="Enumeration"
      value="Unspecified"/>
0184        </RevocationReason>
0185      </RequestPayload>
0186    </BatchItem>
0187  </RequestMessage>
```

```
0188  <ResponseMessage>
0189    <ResponseHeader>
0190      <ProtocolVersion>
0191        <ProtocolVersionMajor type="Integer" value="1"/>
0192        <ProtocolVersionMinor type="Integer" value="2"/>
0193      </ProtocolVersion>
0194      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0195      <BatchCount type="Integer" value="1"/>
0196    </ResponseHeader>
0197    <BatchItem>
0198      <Operation type="Enumeration" value="Revoke"/>
0199      <ResultStatus type="Enumeration" value="Success"/>
0200      <ResponsePayload>
0201        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0202      </ResponsePayload>
0203    </BatchItem>
0204  </ResponseMessage>
```

```
      # TIME 5
0205  <RequestMessage>
0206    <RequestHeader>
0207      <ProtocolVersion>
0208        <ProtocolVersionMajor type="Integer" value="1"/>
0209        <ProtocolVersionMinor type="Integer" value="2"/>
0210      </ProtocolVersion>
0211      <BatchCount type="Integer" value="1"/>
0212    </RequestHeader>
0213    <BatchItem>
0214      <Operation type="Enumeration" value="Destroy"/>
0215      <RequestPayload>
0216        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0217      </RequestPayload>
0218    </BatchItem>
```

```
0219 </RequestMessage>
0220 <ResponseMessage>
0221   <ResponseHeader>
0222     <ProtocolVersion>
0223       <ProtocolVersionMajor type="Integer" value="1"/>
0224       <ProtocolVersionMinor type="Integer" value="2"/>
0225     </ProtocolVersion>
0226     <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0227     <BatchCount type="Integer" value="1"/>
0228   </ResponseHeader>
0229   <BatchItem>
0230     <Operation type="Enumeration" value="Destroy"/>
0231     <ResultStatus type="Enumeration" value="Success"/>
0232     <ResponsePayload>
0233       <UniqueIdentifier type="TextString"
       value="$UNIQUE_IDENTIFIER_0"/>
0234     </ResponsePayload>
0235   </BatchItem>
0236 </ResponseMessage>
```

186

187 ### 3.2.3 CS-AC-M-3-12 - Sign and Signature Verify with Known Asymmetric
188 Key

189 Register an asymmetric key and perform sign and signature verify using the asymmetric key.

```
     # TIME 0
0001 <RequestMessage>
0002   <RequestHeader>
0003     <ProtocolVersion>
0004       <ProtocolVersionMajor type="Integer" value="1"/>
0005       <ProtocolVersionMinor type="Integer" value="2"/>
0006     </ProtocolVersion>
0007     <BatchCount type="Integer" value="1"/>
0008   </RequestHeader>
0009   <BatchItem>
0010     <Operation type="Enumeration" value="Register"/>
0011     <RequestPayload>
0012       <ObjectType type="Enumeration" value="PrivateKey"/>
0013       <TemplateAttribute>
0014         <Attribute>
0015           <AttributeName type="TextString" value="Cryptographic
       Usage Mask"/>
0016           <AttributeValue type="Integer" value="Sign"/>
0017         </Attribute>
0018         <Attribute>
0019           <AttributeName type="TextString" value="x-ID"/>
0020           <AttributeValue type="TextString" value="CS-AC-M-3-12-
       prikey1"/>
0021         </Attribute>
0022         <Attribute>
0023           <AttributeName type="TextString" value="Activation Date"/>
0024           <AttributeValue type="DateTime" value="$NOW-3600"/>
0025         </Attribute>
0026         <Attribute>
0027           <AttributeName type="TextString" value="Cryptographic
       Parameters"/>
0028           <AttributeValue>
```

```
0029              <PaddingMethod type="Enumeration" value="PSS"/>
0030              <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0031              <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0032            </AttributeValue>
0033          </Attribute>
0034        </TemplateAttribute>
0035        <PrivateKey>
0036          <KeyBlock>
0037            <KeyFormatType type="Enumeration" value="PKCS_1"/>
0038            <KeyValue>
0039              <KeyMaterial type="ByteString"
value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353
57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483
46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa
2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650
89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c
795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f
91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281
5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050
203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a
7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f
a74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b
2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0
e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a
a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e
3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78
965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8
c3cdc2464744a793713dafb9f1dbc799ff96423fecd3cba794286bce920f4b5c183f
99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967
4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c
ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064
b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e
59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4
990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766
b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab
7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0
e94ad1ee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db
e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa
e1ebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2
7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eaefa922fd75d5b16b1a5
61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bff1a85a72
6a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171
666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520
a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a
1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d34941
7e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f812
9c32341a8b44f"/>
0040              </KeyValue>
0041              <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0042              <CryptographicLength type="Integer" value="2048"/>
0043            </KeyBlock>
0044          </PrivateKey>
0045        </RequestPayload>
0046      </BatchItem>
0047    </RequestMessage>
0048    <ResponseMessage>
0049      <ResponseHeader>
0050        <ProtocolVersion>
```

```
0051        <ProtocolVersionMajor type="Integer" value="1"/>
0052        <ProtocolVersionMinor type="Integer" value="2"/>
0053      </ProtocolVersion>
0054      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0055      <BatchCount type="Integer" value="1"/>
0056    </ResponseHeader>
0057    <BatchItem>
0058      <Operation type="Enumeration" value="Register"/>
0059      <ResultStatus type="Enumeration" value="Success"/>
0060      <ResponsePayload>
0061        <UniqueIdentifier type="TextString"
value="$UNIQUE IDENTIFIER 0"/>
0062      </ResponsePayload>
0063    </BatchItem>
0064  </ResponseMessage>
```

```
    # TIME 1
0065  <RequestMessage>
0066    <RequestHeader>
0067      <ProtocolVersion>
0068        <ProtocolVersionMajor type="Integer" value="1"/>
0069        <ProtocolVersionMinor type="Integer" value="2"/>
0070      </ProtocolVersion>
0071      <BatchCount type="Integer" value="1"/>
0072    </RequestHeader>
0073    <BatchItem>
0074      <Operation type="Enumeration" value="Register"/>
0075      <RequestPayload>
0076        <ObjectType type="Enumeration" value="PublicKey"/>
0077        <TemplateAttribute>
0078          <Attribute>
0079            <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0080            <AttributeValue type="Integer" value="Verify"/>
0081          </Attribute>
0082          <Attribute>
0083            <AttributeName type="TextString" value="x-ID"/>
0084            <AttributeValue type="TextString" value="CS-AC-M-3-12-
pubkey1"/>
0085          </Attribute>
0086          <Attribute>
0087            <AttributeName type="TextString" value="Activation Date"/>
0088            <AttributeValue type="DateTime" value="$NOW-3600"/>
0089          </Attribute>
0090          <Attribute>
0091            <AttributeValue>
0092              <PaddingMethod type="Enumeration" value="PSS"/>
0093              <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0094              <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0095            </AttributeValue>
0096          </Attribute>
0097        </TemplateAttribute>
0098        <PublicKey>
0099          <KeyBlock>
0100            <KeyFormatType type="Enumeration" value="PKCS_1"/>
0101            <KeyValue>
0102              <KeyMaterial type="ByteString"
value="3082010a0282010100ab7f161c0042496ccd6c6d4dadb91997343535777600
03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b
```

```
8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89
b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981
35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328
abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013
da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612
a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010
001"/>
0103            </KeyValue>
0104            <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0105            <CryptographicLength type="Integer" value="2048"/>
0106          </KeyBlock>
0107        </PublicKey>
0108      </RequestPayload>
0109    </BatchItem>
0110  </RequestMessage>
```

```
0111  <ResponseMessage>
0112    <ResponseHeader>
0113      <ProtocolVersion>
0114        <ProtocolVersionMajor type="Integer" value="1"/>
0115        <ProtocolVersionMinor type="Integer" value="2"/>
0116      </ProtocolVersion>
0117      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0118      <BatchCount type="Integer" value="1"/>
0119    </ResponseHeader>
0120    <BatchItem>
0121      <Operation type="Enumeration" value="Register"/>
0122      <ResultStatus type="Enumeration" value="Success"/>
0123      <ResponsePayload>
0124        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_1"/>
0125      </ResponsePayload>
0126    </BatchItem>
0127  </ResponseMessage>
```

```
      # TIME 2
0128  <RequestMessage>
0129    <RequestHeader>
0130      <ProtocolVersion>
0131        <ProtocolVersionMajor type="Integer" value="1"/>
0132        <ProtocolVersionMinor type="Integer" value="2"/>
0133      </ProtocolVersion>
0134      <BatchCount type="Integer" value="1"/>
0135    </RequestHeader>
0136    <BatchItem>
0137      <Operation type="Enumeration" value="Sign"/>
0138      <RequestPayload>
0139        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0140        <Data type="ByteString"
      value="0102030405060708091011121314151 6"/>
0141      </RequestPayload>
0142    </BatchItem>
0143  </RequestMessage>
```

```
0144  <ResponseMessage>
0145    <ResponseHeader>
0146      <ProtocolVersion>
0147        <ProtocolVersionMajor type="Integer" value="1"/>
0148        <ProtocolVersionMinor type="Integer" value="2"/>
0149      </ProtocolVersion>
```

```
      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
      <BatchCount type="Integer" value="1"/>
    </ResponseHeader>
    <BatchItem>
      <Operation type="Enumeration" value="Sign"/>
      <ResultStatus type="Enumeration" value="Success"/>
      <ResponsePayload>
        <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
        <SignatureData type="ByteString" value="$SIGNATURE_DATA"/>
      </ResponsePayload>
    </BatchItem>
</ResponseMessage>
```

```
# TIME 3
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="SignatureVerify"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
      <CryptographicParameters>
      <PaddingMethod type="Enumeration" value="PSS"/>
      <HashingAlgorithm type="Enumeration" value="SHA_256"/>
      <CryptographicAlgorithm type="Enumeration" value="RSA"/>
      </CryptographicParameters>
      <Data type="ByteString"
value="0102030405060708091011121314151 6"/>
      <SignatureData type="ByteString" value="$SIGNATURE_DATA"/>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="SignatureVerify"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
      <ValidityIndicator type="Enumeration" value="Valid"/>
    </ResponsePayload>
  </BatchItem>
</ResponseMessage>
```

```
# TIME 4
```

```
        # Check that changing the hashing algorithm causes the signature
        verify
        # to fail
0202    <RequestMessage>
0203      <RequestHeader>
0204        <ProtocolVersion>
0205          <ProtocolVersionMajor type="Integer" value="1"/>
0206          <ProtocolVersionMinor type="Integer" value="2"/>
0207        </ProtocolVersion>
0208        <BatchCount type="Integer" value="1"/>
0209      </RequestHeader>
0210      <BatchItem>
0211        <Operation type="Enumeration" value="SignatureVerify"/>
0212        <RequestPayload>
0213          <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_1"/>
0214          <CryptographicParameters>
0215          <PaddingMethod type="Enumeration" value="PSS"/>
0216          <HashingAlgorithm type="Enumeration" value="SHA_1"/>
0217          <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0218          </CryptographicParameters>
0219          <Data type="ByteString"
        value="0102030405060708091011121314151 6"/>
0220          <SignatureData type="ByteString" value="$SIGNATURE_DATA"/>
0221        </RequestPayload>
0222      </BatchItem>
0223    </RequestMessage>
0224    <ResponseMessage>
0225      <ResponseHeader>
0226        <ProtocolVersion>
0227          <ProtocolVersionMajor type="Integer" value="1"/>
0228          <ProtocolVersionMinor type="Integer" value="2"/>
0229        </ProtocolVersion>
0230        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0231        <BatchCount type="Integer" value="1"/>
0232      </ResponseHeader>
0233      <BatchItem>
0234        <Operation type="Enumeration" value="SignatureVerify"/>
0235        <ResultStatus type="Enumeration" value="Success"/>
0236        <ResponsePayload>
0237          <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_1"/>
0238          <ValidityIndicator type="Enumeration" value="Invalid"/>
0239        </ResponsePayload>
0240      </BatchItem>
0241    </ResponseMessage>
        # TIME 5
0242    <RequestMessage>
0243      <RequestHeader>
0244        <ProtocolVersion>
0245          <ProtocolVersionMajor type="Integer" value="1"/>
0246          <ProtocolVersionMinor type="Integer" value="2"/>
0247        </ProtocolVersion>
0248        <BatchCount type="Integer" value="1"/>
0249      </RequestHeader>
0250      <BatchItem>
0251        <Operation type="Enumeration" value="Revoke"/>
0252        <RequestPayload>
```

```
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
      <RevocationReason>
        <RevocationReasonCode type="Enumeration"
value="Unspecified"/>
      </RevocationReason>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
    </ResponsePayload>
  </BatchItem>
</ResponseMessage>
```

```
# TIME 6
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString"
```

```
value="$UNIQUE_IDENTIFIER_0"/>
    </ResponsePayload>
  </BatchItem>
</ResponseMessage>
```

```
# TIME 7
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
      <RevocationReason>
        <RevocationReasonCode type="Enumeration"
value="Unspecified"/>
      </RevocationReason>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
    </ResponsePayload>
  </BatchItem>
</ResponseMessage>
```

```
# TIME 8
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
    </RequestPayload>
```

```
0357    </BatchItem>
0358  </RequestMessage>
```

```
0359  <ResponseMessage>
0360    <ResponseHeader>
0361      <ProtocolVersion>
0362        <ProtocolVersionMajor type="Integer" value="1"/>
0363        <ProtocolVersionMinor type="Integer" value="2"/>
0364      </ProtocolVersion>
0365      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0366      <BatchCount type="Integer" value="1"/>
0367    </ResponseHeader>
0368    <BatchItem>
0369      <Operation type="Enumeration" value="Destroy"/>
0370      <ResultStatus type="Enumeration" value="Success"/>
0371      <ResponsePayload>
0372        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_1"/>
0373      </ResponsePayload>
0374    </BatchItem>
0375  </ResponseMessage>
```

190

191 3.2.4 CS-AC-M-4-12 - MAC with Known Key

192 Register a key and perform MAC operations using the key.

```
      # TIME 0
0001  <RequestMessage>
0002    <RequestHeader>
0003      <ProtocolVersion>
0004        <ProtocolVersionMajor type="Integer" value="1"/>
0005        <ProtocolVersionMinor type="Integer" value="2"/>
0006      </ProtocolVersion>
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="Register"/>
0011      <RequestPayload>
0012        <ObjectType type="Enumeration" value="SymmetricKey"/>
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
        Usage Mask"/>
0016            <AttributeValue type="Integer" value="Encrypt Decrypt
        MACGenerate MACVerify"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="x-ID"/>
0020            <AttributeValue type="TextString" value="CS-AC-M-4-12"/>
0021          </Attribute>
0022          <Attribute>
0023            <AttributeName type="TextString" value="Activation Date"/>
0024            <AttributeValue type="DateTime" value="$NOW-3600"/>
0025          </Attribute>
0026          <Attribute>
0027            <AttributeName type="TextString" value="Cryptographic
        Parameters"/>
0028            <AttributeValue>
```

```
0029              <CryptographicAlgorithm type="Enumeration"
      value="HMAC_SHA256"/>
0030            </AttributeValue>
0031          </Attribute>
0032        </TemplateAttribute>
0033        <SymmetricKey>
0034          <KeyBlock>
0035            <KeyFormatType type="Enumeration" value="Raw"/>
0036            <KeyValue>
0037              <KeyMaterial type="ByteString"
      value="0123456789abcdef0123456789abcdef"/>
0038            </KeyValue>
0039            <CryptographicAlgorithm type="Enumeration" value="AES"/>
0040            <CryptographicLength type="Integer" value="128"/>
0041          </KeyBlock>
0042        </SymmetricKey>
0043      </RequestPayload>
0044    </BatchItem>
0045  </RequestMessage>
0046  <ResponseMessage>
0047    <ResponseHeader>
0048      <ProtocolVersion>
0049        <ProtocolVersionMajor type="Integer" value="1"/>
0050        <ProtocolVersionMinor type="Integer" value="2"/>
0051      </ProtocolVersion>
0052      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0053      <BatchCount type="Integer" value="1"/>
0054    </ResponseHeader>
0055    <BatchItem>
0056      <Operation type="Enumeration" value="Register"/>
0057      <ResultStatus type="Enumeration" value="Success"/>
0058      <ResponsePayload>
0059        <UniqueIdentifier type="TextString"
      value="$UNIQUE IDENTIFIER 0"/>
0060      </ResponsePayload>
0061    </BatchItem>
0062  </ResponseMessage>
      # TIME 1
0063  <RequestMessage>
0064    <RequestHeader>
0065      <ProtocolVersion>
0066        <ProtocolVersionMajor type="Integer" value="1"/>
0067        <ProtocolVersionMinor type="Integer" value="2"/>
0068      </ProtocolVersion>
0069      <BatchCount type="Integer" value="1"/>
0070    </RequestHeader>
0071    <BatchItem>
0072      <Operation type="Enumeration" value="MAC"/>
0073      <RequestPayload>
0074        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0075        <Data type="ByteString"
      value="0102030405060708091011121314151 6"/>
0076      </RequestPayload>
0077    </BatchItem>
0078  </RequestMessage>
0079  <ResponseMessage>
0080    <ResponseHeader>
```

```
0081        <ProtocolVersion>
0082          <ProtocolVersionMajor type="Integer" value="1"/>
0083          <ProtocolVersionMinor type="Integer" value="2"/>
0084        </ProtocolVersion>
0085        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0086        <BatchCount type="Integer" value="1"/>
0087      </ResponseHeader>
0088      <BatchItem>
0089        <Operation type="Enumeration" value="MAC"/>
0090        <ResultStatus type="Enumeration" value="Success"/>
0091        <ResponsePayload>
0092          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0093          <MACData type="ByteString"
          value="c911e78196d64c30f631bb079ea37b97a95936d4da764d6a171df030c895e
          cf9"/>
0094        </ResponsePayload>
0095      </BatchItem>
0096    </ResponseMessage>
```

```
        # TIME 2
0097    <RequestMessage>
0098      <RequestHeader>
0099        <ProtocolVersion>
0100          <ProtocolVersionMajor type="Integer" value="1"/>
0101          <ProtocolVersionMinor type="Integer" value="2"/>
0102        </ProtocolVersion>
0103        <BatchCount type="Integer" value="1"/>
0104      </RequestHeader>
0105      <BatchItem>
0106        <Operation type="Enumeration" value="Revoke"/>
0107        <RequestPayload>
0108          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0109          <RevocationReason>
0110            <RevocationReasonCode type="Enumeration"
          value="Unspecified"/>
0111          </RevocationReason>
0112        </RequestPayload>
0113      </BatchItem>
0114    </RequestMessage>
```

```
0115    <ResponseMessage>
0116      <ResponseHeader>
0117        <ProtocolVersion>
0118          <ProtocolVersionMajor type="Integer" value="1"/>
0119          <ProtocolVersionMinor type="Integer" value="2"/>
0120        </ProtocolVersion>
0121        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0122        <BatchCount type="Integer" value="1"/>
0123      </ResponseHeader>
0124      <BatchItem>
0125        <Operation type="Enumeration" value="Revoke"/>
0126        <ResultStatus type="Enumeration" value="Success"/>
0127        <ResponsePayload>
0128          <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0129        </ResponsePayload>
0130      </BatchItem>
0131    </ResponseMessage>
```

```
      # TIME 3
0132  <RequestMessage>
0133    <RequestHeader>
0134      <ProtocolVersion>
0135        <ProtocolVersionMajor type="Integer" value="1"/>
0136        <ProtocolVersionMinor type="Integer" value="2"/>
0137      </ProtocolVersion>
0138      <BatchCount type="Integer" value="1"/>
0139    </RequestHeader>
0140    <BatchItem>
0141      <Operation type="Enumeration" value="Destroy"/>
0142      <RequestPayload>
0143        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0144      </RequestPayload>
0145    </BatchItem>
0146  </RequestMessage>
```

```
0147  <ResponseMessage>
0148    <ResponseHeader>
0149      <ProtocolVersion>
0150        <ProtocolVersionMajor type="Integer" value="1"/>
0151        <ProtocolVersionMinor type="Integer" value="2"/>
0152      </ProtocolVersion>
0153      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0154      <BatchCount type="Integer" value="1"/>
0155    </ResponseHeader>
0156    <BatchItem>
0157      <Operation type="Enumeration" value="Destroy"/>
0158      <ResultStatus type="Enumeration" value="Success"/>
0159      <ResponsePayload>
0160        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0161      </ResponsePayload>
0162    </BatchItem>
0163  </ResponseMessage>
```

193

194 3.2.5 CS-AC-M-5-12 - MAC Verify with Known Key

195 Register a key and perform MAC verification operations using the key.

196

```
      # TIME 0
0001  <RequestMessage>
0002    <RequestHeader>
0003      <ProtocolVersion>
0004        <ProtocolVersionMajor type="Integer" value="1"/>
0005        <ProtocolVersionMinor type="Integer" value="2"/>
0006      </ProtocolVersion>
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="Register"/>
0011      <RequestPayload>
0012        <ObjectType type="Enumeration" value="SymmetricKey"/>
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
```

```
Usage Mask"/>
0016            <AttributeValue type="Integer" value="Encrypt Decrypt
MACGenerate MACVerify"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="x-ID"/>
0020            <AttributeValue type="TextString" value="CS-AC-M-5-12"/>
0021          </Attribute>
0022          <Attribute>
0023            <AttributeName type="TextString" value="Activation Date"/>
0024            <AttributeValue type="DateTime" value="$NOW-3600"/>
0025          </Attribute>
0026          <Attribute>
0027            <AttributeName type="TextString" value="Cryptographic
Parameters"/>
0028            <AttributeValue>
0029              <CryptographicAlgorithm type="Enumeration"
value="HMAC_SHA256"/>
0030            </AttributeValue>
0031          </Attribute>
0032        </TemplateAttribute>
0033        <SymmetricKey>
0034          <KeyBlock>
0035            <KeyFormatType type="Enumeration" value="Raw"/>
0036            <KeyValue>
0037              <KeyMaterial type="ByteString"
value="0123456789abcdef0123456789abcdef"/>
0038            </KeyValue>
0039            <CryptographicAlgorithm type="Enumeration" value="AES"/>
0040            <CryptographicLength type="Integer" value="128"/>
0041          </KeyBlock>
0042        </SymmetricKey>
0043      </RequestPayload>
0044    </BatchItem>
0045  </RequestMessage>
0046  <ResponseMessage>
0047    <ResponseHeader>
0048      <ProtocolVersion>
0049        <ProtocolVersionMajor type="Integer" value="1"/>
0050        <ProtocolVersionMinor type="Integer" value="2"/>
0051      </ProtocolVersion>
0052      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0053      <BatchCount type="Integer" value="1"/>
0054    </ResponseHeader>
0055    <BatchItem>
0056      <Operation type="Enumeration" value="Register"/>
0057      <ResultStatus type="Enumeration" value="Success"/>
0058      <ResponsePayload>
0059        <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0060      </ResponsePayload>
0061    </BatchItem>
0062  </ResponseMessage>
      # TIME 1
0063  <RequestMessage>
0064    <RequestHeader>
0065      <ProtocolVersion>
0066        <ProtocolVersionMajor type="Integer" value="1"/>
```

```
0067        <ProtocolVersionMinor type="Integer" value="2"/>
0068      </ProtocolVersion>
0069      <BatchCount type="Integer" value="1"/>
0070    </RequestHeader>
0071    <BatchItem>
0072      <Operation type="Enumeration" value="MACVerify"/>
0073      <RequestPayload>
0074        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0075        <Data type="ByteString"
        value="0102030405060708091011121314151 6"/>
0076        <MACData type="ByteString"
        value="c911e78196d64c30f631bb079ea37b97a95936d4da764d6a171df030c895e
        cf9"/>
0077      </RequestPayload>
0078    </BatchItem>
0079  </RequestMessage>
0080  <ResponseMessage>
0081    <ResponseHeader>
0082      <ProtocolVersion>
0083        <ProtocolVersionMajor type="Integer" value="1"/>
0084        <ProtocolVersionMinor type="Integer" value="2"/>
0085      </ProtocolVersion>
0086      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0087      <BatchCount type="Integer" value="1"/>
0088    </ResponseHeader>
0089    <BatchItem>
0090      <Operation type="Enumeration" value="MACVerify"/>
0091      <ResultStatus type="Enumeration" value="Success"/>
0092      <ResponsePayload>
0093        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0094        <ValidityIndicator type="Enumeration" value="Valid"/>
0095      </ResponsePayload>
0096    </BatchItem>
0097  </ResponseMessage>
      # TIME 2
0098  <RequestMessage>
0099    <RequestHeader>
0100      <ProtocolVersion>
0101        <ProtocolVersionMajor type="Integer" value="1"/>
0102        <ProtocolVersionMinor type="Integer" value="2"/>
0103      </ProtocolVersion>
0104      <BatchCount type="Integer" value="1"/>
0105    </RequestHeader>
0106    <BatchItem>
0107      <Operation type="Enumeration" value="Revoke"/>
0108      <RequestPayload>
0109        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0110        <RevocationReason>
0111          <RevocationReasonCode type="Enumeration"
        value="Unspecified"/>
0112        </RevocationReason>
0113      </RequestPayload>
0114    </BatchItem>
0115  </RequestMessage>
0116  <ResponseMessage>
```

```
0117    <ResponseHeader>
0118      <ProtocolVersion>
0119        <ProtocolVersionMajor type="Integer" value="1"/>
0120        <ProtocolVersionMinor type="Integer" value="2"/>
0121      </ProtocolVersion>
0122      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0123      <BatchCount type="Integer" value="1"/>
0124    </ResponseHeader>
0125    <BatchItem>
0126      <Operation type="Enumeration" value="Revoke"/>
0127      <ResultStatus type="Enumeration" value="Success"/>
0128      <ResponsePayload>
0129        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0130      </ResponsePayload>
0131    </BatchItem>
0132  </ResponseMessage>
```

```
        # TIME 3
0133  <RequestMessage>
0134    <RequestHeader>
0135      <ProtocolVersion>
0136        <ProtocolVersionMajor type="Integer" value="1"/>
0137        <ProtocolVersionMinor type="Integer" value="2"/>
0138      </ProtocolVersion>
0139      <BatchCount type="Integer" value="1"/>
0140    </RequestHeader>
0141    <BatchItem>
0142      <Operation type="Enumeration" value="Destroy"/>
0143      <RequestPayload>
0144        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0145      </RequestPayload>
0146    </BatchItem>
0147  </RequestMessage>
```

```
0148  <ResponseMessage>
0149    <ResponseHeader>
0150      <ProtocolVersion>
0151        <ProtocolVersionMajor type="Integer" value="1"/>
0152        <ProtocolVersionMinor type="Integer" value="2"/>
0153      </ProtocolVersion>
0154      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0155      <BatchCount type="Integer" value="1"/>
0156    </ResponseHeader>
0157    <BatchItem>
0158      <Operation type="Enumeration" value="Destroy"/>
0159      <ResultStatus type="Enumeration" value="Success"/>
0160      <ResponsePayload>
0161        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0162      </ResponsePayload>
0163    </BatchItem>
0164  </ResponseMessage>
```

197

198 3.2.6 CS-AC-M-6-12 - MAC and MAC Verify with Known Key

199 MAC and MAC Verify with Known Key.

200

```
      # TIME 0
0001  <RequestMessage>
0002    <RequestHeader>
0003      <ProtocolVersion>
0004        <ProtocolVersionMajor type="Integer" value="1"/>
0005        <ProtocolVersionMinor type="Integer" value="2"/>
0006      </ProtocolVersion>
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="Register"/>
0011      <RequestPayload>
0012        <ObjectType type="Enumeration" value="SymmetricKey"/>
0013        <TemplateAttribute>
0014          <Attribute>
0015            <AttributeName type="TextString" value="Cryptographic
          Usage Mask"/>
0016            <AttributeValue type="Integer" value="Encrypt Decrypt
          MACGenerate MACVerify"/>
0017          </Attribute>
0018          <Attribute>
0019            <AttributeName type="TextString" value="x-ID"/>
0020            <AttributeValue type="TextString" value="CS-AC-M-6-12"/>
0021          </Attribute>
0022          <Attribute>
0023            <AttributeName type="TextString" value="Activation Date"/>
0024            <AttributeValue type="DateTime" value="$NOW-3600"/>
0025          </Attribute>
0026          <Attribute>
0027            <AttributeName type="TextString" value="Cryptographic
          Parameters"/>
0028            <AttributeValue>
0029              <CryptographicAlgorithm type="Enumeration"
          value="HMAC_SHA256"/>
0030            </AttributeValue>
0031          </Attribute>
0032        </TemplateAttribute>
0033        <SymmetricKey>
0034          <KeyBlock>
0035            <KeyFormatType type="Enumeration" value="Raw"/>
0036            <KeyValue>
0037              <KeyMaterial type="ByteString"
          value="0123456789abcdef0123456789abcdef"/>
0038            </KeyValue>
0039            <CryptographicAlgorithm type="Enumeration" value="AES"/>
0040            <CryptographicLength type="Integer" value="128"/>
0041          </KeyBlock>
0042        </SymmetricKey>
0043      </RequestPayload>
0044    </BatchItem>
0045  </RequestMessage>
0046  <ResponseMessage>
0047    <ResponseHeader>
0048      <ProtocolVersion>
0049        <ProtocolVersionMajor type="Integer" value="1"/>
0050        <ProtocolVersionMinor type="Integer" value="2"/>
```

```
0051      </ProtocolVersion>
0052      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0053      <BatchCount type="Integer" value="1"/>
0054    </ResponseHeader>
0055    <BatchItem>
0056      <Operation type="Enumeration" value="Register"/>
0057      <ResultStatus type="Enumeration" value="Success"/>
0058      <ResponsePayload>
0059        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0060      </ResponsePayload>
0061    </BatchItem>
0062  </ResponseMessage>
```

```
        # TIME 1
0063  <RequestMessage>
0064    <RequestHeader>
0065      <ProtocolVersion>
0066        <ProtocolVersionMajor type="Integer" value="1"/>
0067        <ProtocolVersionMinor type="Integer" value="2"/>
0068      </ProtocolVersion>
0069      <BatchCount type="Integer" value="1"/>
0070    </RequestHeader>
0071    <BatchItem>
0072      <Operation type="Enumeration" value="MAC"/>
0073      <RequestPayload>
0074        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0075        <Data type="ByteString"
        value="0102030405060708091011121314151 6"/>
0076      </RequestPayload>
0077    </BatchItem>
0078  </RequestMessage>
```

```
0079  <ResponseMessage>
0080    <ResponseHeader>
0081      <ProtocolVersion>
0082        <ProtocolVersionMajor type="Integer" value="1"/>
0083        <ProtocolVersionMinor type="Integer" value="2"/>
0084      </ProtocolVersion>
0085      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0086      <BatchCount type="Integer" value="1"/>
0087    </ResponseHeader>
0088    <BatchItem>
0089      <Operation type="Enumeration" value="MAC"/>
0090      <ResultStatus type="Enumeration" value="Success"/>
0091      <ResponsePayload>
0092        <UniqueIdentifier type="TextString"
        value="$UNIQUE_IDENTIFIER_0"/>
0093        <MACData type="ByteString"
        value="c911e78196d64c30f631bb079ea37b97a95936d4da764d6a171df030c895e
        cf9"/>
0094      </ResponsePayload>
0095    </BatchItem>
0096  </ResponseMessage>
```

```
        # TIME 2
0097  <RequestMessage>
0098    <RequestHeader>
0099      <ProtocolVersion>
0100        <ProtocolVersionMajor type="Integer" value="1"/>
```

```
0101        <ProtocolVersionMinor type="Integer" value="2"/>
0102      </ProtocolVersion>
0103      <BatchCount type="Integer" value="1"/>
0104    </RequestHeader>
0105    <BatchItem>
0106      <Operation type="Enumeration" value="MACVerify"/>
0107      <RequestPayload>
0108        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0109        <Data type="ByteString"
      value="0102030405060708091011121314151 6"/>
0110        <MACData type="ByteString" value="$MAC_DATA"/>
0111      </RequestPayload>
0112    </BatchItem>
0113  </RequestMessage>
0114  <ResponseMessage>
0115    <ResponseHeader>
0116      <ProtocolVersion>
0117        <ProtocolVersionMajor type="Integer" value="1"/>
0118        <ProtocolVersionMinor type="Integer" value="2"/>
0119      </ProtocolVersion>
0120      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0121      <BatchCount type="Integer" value="1"/>
0122    </ResponseHeader>
0123    <BatchItem>
0124      <Operation type="Enumeration" value="MACVerify"/>
0125      <ResultStatus type="Enumeration" value="Success"/>
0126      <ResponsePayload>
0127        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0128        <ValidityIndicator type="Enumeration" value="Valid"/>
0129      </ResponsePayload>
0130    </BatchItem>
0131  </ResponseMessage>
      # TIME 3
0132  <RequestMessage>
0133    <RequestHeader>
0134      <ProtocolVersion>
0135        <ProtocolVersionMajor type="Integer" value="1"/>
0136        <ProtocolVersionMinor type="Integer" value="2"/>
0137      </ProtocolVersion>
0138      <BatchCount type="Integer" value="1"/>
0139    </RequestHeader>
0140    <BatchItem>
0141      <Operation type="Enumeration" value="Revoke"/>
0142      <RequestPayload>
0143        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0144        <RevocationReason>
0145          <RevocationReasonCode type="Enumeration"
      value="Unspecified"/>
0146        </RevocationReason>
0147      </RequestPayload>
0148    </BatchItem>
0149  </RequestMessage>
0150  <ResponseMessage>
0151    <ResponseHeader>
0152      <ProtocolVersion>
```

```
0153        <ProtocolVersionMajor type="Integer" value="1"/>
0154        <ProtocolVersionMinor type="Integer" value="2"/>
0155      </ProtocolVersion>
0156      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0157      <BatchCount type="Integer" value="1"/>
0158    </ResponseHeader>
0159    <BatchItem>
0160      <Operation type="Enumeration" value="Revoke"/>
0161      <ResultStatus type="Enumeration" value="Success"/>
0162      <ResponsePayload>
0163        <UniqueIdentifier type="TextString"
      value="$UNIQUE IDENTIFIER 0"/>
0164      </ResponsePayload>
0165    </BatchItem>
0166  </ResponseMessage>
```

```
      # TIME 4
0167  <RequestMessage>
0168    <RequestHeader>
0169      <ProtocolVersion>
0170        <ProtocolVersionMajor type="Integer" value="1"/>
0171        <ProtocolVersionMinor type="Integer" value="2"/>
0172      </ProtocolVersion>
0173      <BatchCount type="Integer" value="1"/>
0174    </RequestHeader>
0175    <BatchItem>
0176      <Operation type="Enumeration" value="Destroy"/>
0177      <RequestPayload>
0178        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
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="2013-06-21T22:18:59+00:00"/>
0189      <BatchCount type="Integer" value="1"/>
0190    </ResponseHeader>
0191    <BatchItem>
0192      <Operation type="Enumeration" value="Destroy"/>
0193      <ResultStatus type="Enumeration" value="Success"/>
0194      <ResponsePayload>
0195        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_0"/>
0196      </ResponsePayload>
0197    </BatchItem>
0198  </ResponseMessage>
```

201

202 3.2.7 CS-AC-M-7-12 - HASH

203 Hash Data

```
      # 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="Hash"/>
0011      <RequestPayload>
0012        <CryptographicParameters>
0013        <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0014        </CryptographicParameters>
0015        <Data type="ByteString"
        value="0102030405060708091011121314151 6"/>
0016      </RequestPayload>
0017    </BatchItem>
0018  </RequestMessage>
```

```
0019  <ResponseMessage>
0020    <ResponseHeader>
0021      <ProtocolVersion>
0022        <ProtocolVersionMajor type="Integer" value="1"/>
0023        <ProtocolVersionMinor type="Integer" value="2"/>
0024      </ProtocolVersion>
0025      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0026      <BatchCount type="Integer" value="1"/>
0027    </ResponseHeader>
0028    <BatchItem>
0029      <Operation type="Enumeration" value="Hash"/>
0030      <ResultStatus type="Enumeration" value="Success"/>
0031      <ResponsePayload>
0032        <Data type="ByteString"
        value="ad41233d22cf9322e3a7ff49a13da434797abed3bab80950a1a0d4e582b7e
        a72"/>
0033      </ResponsePayload>
0034    </BatchItem>
0035  </ResponseMessage>
```

```
        # TIME 1
0036  <RequestMessage>
0037    <RequestHeader>
0038      <ProtocolVersion>
0039        <ProtocolVersionMajor type="Integer" value="1"/>
0040        <ProtocolVersionMinor type="Integer" value="2"/>
0041      </ProtocolVersion>
0042      <BatchCount type="Integer" value="1"/>
0043    </RequestHeader>
0044    <BatchItem>
0045      <Operation type="Enumeration" value="Hash"/>
0046      <RequestPayload>
0047        <CryptographicParameters>
0048        <HashingAlgorithm type="Enumeration" value="SHA_512"/>
0049        </CryptographicParameters>
0050        <Data type="ByteString"
        value="0102030405060708091011121314151 6"/>
0051      </RequestPayload>
0052    </BatchItem>
0053  </RequestMessage>
```

```
0054  <ResponseMessage>
```

```
0055    <ResponseHeader>
0056      <ProtocolVersion>
0057        <ProtocolVersionMajor type="Integer" value="1"/>
0058        <ProtocolVersionMinor type="Integer" value="2"/>
0059      </ProtocolVersion>
0060      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0061      <BatchCount type="Integer" value="1"/>
0062    </ResponseHeader>
0063    <BatchItem>
0064      <Operation type="Enumeration" value="Hash"/>
0065      <ResultStatus type="Enumeration" value="Success"/>
0066      <ResponsePayload>
0067        <Data type="ByteString"
        value="406a806f76c06b90c8aca278995d4271037f91124ebfaba5475f1f59ee21e
        be3a0cc7f5ca6f2183d360bcc762cef68713de7c6498eb08dc591075ca62f7a0717"
        />
0068      </ResponsePayload>
0069    </BatchItem>
0070  </ResponseMessage>
```

204

205 3.2.8 CS-AC-M-8-12 - Sign and Signature Verify with Known Asymmetric 206 Key Date Checks

207 Register an asymmetric key and perform sign and signature verify using the asymmetric key outside of
208 the valid Process Start Date and Protect Stop Date to confirm the operations fail.

209 The Process Start Date is set to a future date. The Protect Stop Date is set to a past date.

210 This is a modified version of CS-AC-M-3-12.

```
        # TIME 0
0001    <RequestMessage>
0002      <RequestHeader>
0003        <ProtocolVersion>
0004          <ProtocolVersionMajor type="Integer" value="1"/>
0005          <ProtocolVersionMinor type="Integer" value="2"/>
0006        </ProtocolVersion>
0007        <BatchCount type="Integer" value="1"/>
0008      </RequestHeader>
0009      <BatchItem>
0010        <Operation type="Enumeration" value="Register"/>
0011        <RequestPayload>
0012          <ObjectType type="Enumeration" value="PrivateKey"/>
0013          <TemplateAttribute>
0014            <Attribute>
0015              <AttributeName type="TextString" value="Cryptographic
        Usage Mask"/>
0016              <AttributeValue type="Integer" value="Sign"/>
0017            </Attribute>
0018            <Attribute>
0019              <AttributeName type="TextString" value="x-ID"/>
0020              <AttributeValue type="TextString" value="CS-AC-M-8-12-
        prikey1"/>
0021            </Attribute>
0022            <Attribute>
0023              <AttributeName type="TextString" value="Activation Date"/>
0024              <AttributeValue type="DateTime" value="$NOW-3600"/>
0025            </Attribute>
```

```
0026          <Attribute>
0027            <AttributeName type="TextString" value="Process Start
      Date"/>
0028            <AttributeValue type="DateTime" value="$NOW+3600"/>
0029          </Attribute>
0030          <Attribute>
0031            <AttributeName type="TextString" value="Protect Stop
      Date"/>
0032            <AttributeValue type="DateTime" value="$NOW-3600"/>
0033          </Attribute>
0034          <Attribute>
0035            <AttributeName type="TextString" value="Cryptographic
      Parameters"/>
0036            <AttributeValue>
0037              <PaddingMethod type="Enumeration" value="PSS"/>
0038              <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0039              <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0040            </AttributeValue>
0041          </Attribute>
0042        </TemplateAttribute>
0043        <PrivateKey>
0044          <KeyBlock>
0045            <KeyFormatType type="Enumeration" value="PKCS_1"/>
0046            <KeyValue>
0047              <KeyMaterial type="ByteString"
      value="308204a50201000282010100ab7f161c0042496ccd6c6d4dadb9199734353
      57776003acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d746483
      46d75b8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa
      2a6f89b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b650
      89f98135b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c
      795328abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f
      91f013da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c281
      5c3612a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050
      203010001028201003b12455d53c1816516c518493f6398aafa72b17dfa894db888a
      7d48c0a47f62579a4e644f86da711fec850cdd9dbbd17f69a443d2ec1dd60d3c618f
      a74cde5fdafabd6baa26eb0a3adb4def6480fb1218cd3b083e252e885b6f0729f98b
      2144d2b72293e1b11d73393bc41f75b15ee3d7569b4995ed1a14425da4319b7b26b0
      e8fef17c37542ae5c6d5849f87209567f3925a47b016d564859717bc57fcb4522d0a
      a49ce816e5be7b3088193236ec9efff140858045b73c5d79baf38f7c67f04c5dcf0e
      3806ad982d1259058c3473e847179a878f2c6b3bd968fb99ea46e9185892f3676e78
      965c2aed4877ba3917df07c5e927474f19e764ba61dc38d63bf2902818100d5c69c8
      c3cdc2464744a793713dafb9f1dbc799ff96423fecd3cba794286bce920f4b5c183f
      99ee9028db6212c6277c4c8297fcfbce7f7c24ca4c51fc7182fb8f4019fb1d565967
      4c5cbe6d5fa992051341760cd00735729a070a9e54d342beba8ef47ee82d3a01b04c
      ec4a00d4ddb41e35116fc221e854b43a696c0e6419b1b02818100cd5ea7702789064
      b673540cbff09356ad80bc3d592812eba47610b9fac6aecefe22acae438459cda74e
      59653d88c04189d34399bf5b14b920e34ef38a7d09fe69593396e8fe735e6f0a6ae4
      990401041d8a406b6fd86a1161e45f95a3eaa5c1012e6662e44f15f335ac971e1766
      b2bb9c985109974141b44d37e1e319820a55f02818100b2871237bf9fad38c3316ab
      7877a6a868063e542a7186d431e8d27c19ac0414584033942e9ff6e2973bb7b2d8b0
      e94ad1ee82158108fbc8664517a5a467fb963014bd5dcc2b4fb087c23039d11920db
      e22fd9f16b4d89e23225cd455adbaf32ef43f185864a36d630309d6853f7714b39aa
      e1ebee3938f87c2707e178c739f9f028181009690bed14b2afaa26d986d592231ee2
      7d71d49065bd2ba1f78157e20229881fd9d23227d0f8479eaefa922fd75d5b16b1a5
      61fa6680b040ca0bdce650b23b917a4b1bb7983a74fad70e1c305cbec2bff1a85a72
      6a1d90260e4f1084f518234dcd3fe770b9520215bd543bb6a4117718754676a34171
      666a79f26e79c149c5aa102818100a0c985a0a0a791a659f99731134c44f37b2e520
      a2cea35800ad27241ed360dfde6e8ca614f12047fd08b76ac4d13c056a0699e2f98a
```

```
1cac91011294d71208f4abab33ba87aa0517f415baca88d6bac006088fa601d34941
7e1f0c9b23affa4d496618dbc024986ed690bbb7b025768ff9df8ac15416f489f812
9c32341a8b44f"/>
0048            </KeyValue>
0049            <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0050            <CryptographicLength type="Integer" value="2048"/>
0051          </KeyBlock>
0052        </PrivateKey>
0053      </RequestPayload>
0054    </BatchItem>
0055  </RequestMessage>
0056  <ResponseMessage>
0057    <ResponseHeader>
0058      <ProtocolVersion>
0059        <ProtocolVersionMajor type="Integer" value="1"/>
0060        <ProtocolVersionMinor type="Integer" value="2"/>
0061      </ProtocolVersion>
0062      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0063      <BatchCount type="Integer" value="1"/>
0064    </ResponseHeader>
0065    <BatchItem>
0066      <Operation type="Enumeration" value="Register"/>
0067      <ResultStatus type="Enumeration" value="Success"/>
0068      <ResponsePayload>
0069        <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0070      </ResponsePayload>
0071    </BatchItem>
0072  </ResponseMessage>
    # TIME 1
0073  <RequestMessage>
0074    <RequestHeader>
0075      <ProtocolVersion>
0076        <ProtocolVersionMajor type="Integer" value="1"/>
0077        <ProtocolVersionMinor type="Integer" value="2"/>
0078      </ProtocolVersion>
0079      <BatchCount type="Integer" value="1"/>
0080    </RequestHeader>
0081    <BatchItem>
0082      <Operation type="Enumeration" value="Register"/>
0083      <RequestPayload>
0084        <ObjectType type="Enumeration" value="PublicKey"/>
0085        <TemplateAttribute>
0086          <Attribute>
0087            <AttributeName type="TextString" value="Cryptographic
Usage Mask"/>
0088            <AttributeValue type="Integer" value="Verify"/>
0089          </Attribute>
0090          <Attribute>
0091            <AttributeName type="TextString" value="x-ID"/>
0092            <AttributeValue type="TextString" value="CS-AC-M-8-12-
pubkey1"/>
0093          </Attribute>
0094          <Attribute>
0095            <AttributeName type="TextString" value="Activation Date"/>
0096            <AttributeValue type="DateTime" value="$NOW-3600"/>
0097          </Attribute>
0098          <Attribute>
```

```
0099            <AttributeName type="TextString" value="Process Start
    Date"/>
0100            <AttributeValue type="DateTime" value="$NOW+3600"/>
0101          </Attribute>
0102          <Attribute>
0103            <AttributeName type="TextString" value="Protect Stop
    Date"/>
0104            <AttributeValue type="DateTime" value="$NOW-3600"/>
0105          </Attribute>
0106          <Attribute>
0107            <AttributeValue>
0108              <PaddingMethod type="Enumeration" value="PSS"/>
0109              <HashingAlgorithm type="Enumeration" value="SHA_256"/>
0110              <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0111            </AttributeValue>
0112          </Attribute>
0113        </TemplateAttribute>
0114        <PublicKey>
0115          <KeyBlock>
0116            <KeyFormatType type="Enumeration" value="PKCS_1"/>
0117            <KeyValue>
0118              <KeyMaterial type="ByteString"
    value="3082010a0282010100ab7f161c0042496ccd6c6d4dadb9199734353577760
    03acf54b7af1e440afb80b64a8755f8002cfeba6b184540a2d66086d74648346d75b
    8d71812b205387c0f6583bc4d7dc7ec114f3b176b7957c422e7d03fc6267fa2a6f89
    b9bee9e60a1d7c2d833e5a5f4bb0b1434f4e795a41100f8aa214900df8b65089f981
    35b1c67b701675abdbc7d5721aac9d14a7f081fcec80b64e8a0ecc8295353c795328
    abf70e1b42e7bb8b7f4e8ac8c810cdb66e3d21126eba8da7d0ca34142cb76f91f013
    da809e9c1b7ae64c54130fbc21d80e9c2cb06c5c8d7cce8946a9ac99b1c2815c3612
    a29a82d73a1f99374fe30e54951662a6eda29c6fc411335d5dc7426b0f6050203010
    001"/>
0119            </KeyValue>
0120            <CryptographicAlgorithm type="Enumeration" value="RSA"/>
0121            <CryptographicLength type="Integer" value="2048"/>
0122          </KeyBlock>
0123        </PublicKey>
0124      </RequestPayload>
0125    </BatchItem>
0126  </RequestMessage>
```

```
0127  <ResponseMessage>
0128    <ResponseHeader>
0129      <ProtocolVersion>
0130        <ProtocolVersionMajor type="Integer" value="1"/>
0131        <ProtocolVersionMinor type="Integer" value="2"/>
0132      </ProtocolVersion>
0133      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0134      <BatchCount type="Integer" value="1"/>
0135    </ResponseHeader>
0136    <BatchItem>
0137      <Operation type="Enumeration" value="Register"/>
0138      <ResultStatus type="Enumeration" value="Success"/>
0139      <ResponsePayload>
0140        <UniqueIdentifier type="TextString"
    value="$UNIQUE_IDENTIFIER_1"/>
0141      </ResponsePayload>
0142    </BatchItem>
0143  </ResponseMessage>
```

```
      # TIME 2
```

```
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Sign"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
      <Data type="ByteString"
value="0102030405060708091011121314151 6"/>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Sign"/>
    <ResultStatus type="Enumeration" value="OperationFailed"/>
    <ResultReason type="Enumeration" value="PermissionDenied"/>
    <ResultMessage type="TextString" value="DENIED"/>
  </BatchItem>
</ResponseMessage>
```

```
# TIME 3
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="SignatureVerify"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_1"/>
      <CryptographicParameters>
      <PaddingMethod type="Enumeration" value="PSS"/>
      <HashingAlgorithm type="Enumeration" value="SHA_256"/>
      <CryptographicAlgorithm type="Enumeration" value="RSA"/>
      </CryptographicParameters>
      <Data type="ByteString"
value="0102030405060708091011121314151 6"/>
      <SignatureData type="ByteString"
value="2925ebf8c6c9d0585c36a44491dd28f8ffd1098d2275a505a0eba7af452e9
496472fd5c4a515d1c0db16c7c59ef76863b571cbf498fb8178ffeb75667e6e51b9b
```

```
9bbf09d55bba54b42acb947aa5a81dc62751727d7cad4616c0c0bf1dd666f8266f24
262c5fa9cbbdc424ef5f5e345e633d111e66eb4afc4001bb02e158b2d5d4573c6146
55f21a688bee0e9dbde6a58324c08f42ae69697e0c51803f9de6b3df242d2915d9b1
a8110ad28143ab7855ef92ede48971b484172de3b0b8957f493a74b3372ee2200f22
33607735f90d0b180968ab20d74841fd3dba4fb1f225ea5c6c87f99c2a238db72a53
6e68be202a092cd032337d451477e568f9a48b638cb"/>
0195        </RequestPayload>
0196      </BatchItem>
0197    </RequestMessage>
0198    <ResponseMessage>
0199      <ResponseHeader>
0200        <ProtocolVersion>
0201          <ProtocolVersionMajor type="Integer" value="1"/>
0202          <ProtocolVersionMinor type="Integer" value="2"/>
0203        </ProtocolVersion>
0204        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0205        <BatchCount type="Integer" value="1"/>
0206      </ResponseHeader>
0207      <BatchItem>
0208        <Operation type="Enumeration" value="SignatureVerify"/>
0209        <ResultStatus type="Enumeration" value="OperationFailed"/>
0210        <ResultReason type="Enumeration" value="PermissionDenied"/>
0211        <ResultMessage type="TextString" value="DENIED"/>
0212      </BatchItem>
0213    </ResponseMessage>
    # TIME 4
0214    <RequestMessage>
0215      <RequestHeader>
0216        <ProtocolVersion>
0217          <ProtocolVersionMajor type="Integer" value="1"/>
0218          <ProtocolVersionMinor type="Integer" value="2"/>
0219        </ProtocolVersion>
0220        <BatchCount type="Integer" value="1"/>
0221      </RequestHeader>
0222      <BatchItem>
0223        <Operation type="Enumeration" value="Revoke"/>
0224        <RequestPayload>
0225          <UniqueIdentifier type="TextString"
value="$UNIQUE_IDENTIFIER_0"/>
0226          <RevocationReason>
0227            <RevocationReasonCode type="Enumeration"
value="Unspecified"/>
0228          </RevocationReason>
0229        </RequestPayload>
0230      </BatchItem>
0231    </RequestMessage>
0232    <ResponseMessage>
0233      <ResponseHeader>
0234        <ProtocolVersion>
0235          <ProtocolVersionMajor type="Integer" value="1"/>
0236          <ProtocolVersionMinor type="Integer" value="2"/>
0237        </ProtocolVersion>
0238        <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0239        <BatchCount type="Integer" value="1"/>
0240      </ResponseHeader>
0241      <BatchItem>
0242        <Operation type="Enumeration" value="Revoke"/>
0243        <ResultStatus type="Enumeration" value="Success"/>
```

```
0244      <ResponsePayload>
0245        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0246      </ResponsePayload>
0247    </BatchItem>
0248  </ResponseMessage>
```

```
          # TIME 5
0249  <RequestMessage>
0250    <RequestHeader>
0251      <ProtocolVersion>
0252        <ProtocolVersionMajor type="Integer" value="1"/>
0253        <ProtocolVersionMinor type="Integer" value="2"/>
0254      </ProtocolVersion>
0255      <BatchCount type="Integer" value="1"/>
0256    </RequestHeader>
0257    <BatchItem>
0258      <Operation type="Enumeration" value="Destroy"/>
0259      <RequestPayload>
0260        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0261      </RequestPayload>
0262    </BatchItem>
0263  </RequestMessage>
```

```
0264  <ResponseMessage>
0265    <ResponseHeader>
0266      <ProtocolVersion>
0267        <ProtocolVersionMajor type="Integer" value="1"/>
0268        <ProtocolVersionMinor type="Integer" value="2"/>
0269      </ProtocolVersion>
0270      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0271      <BatchCount type="Integer" value="1"/>
0272    </ResponseHeader>
0273    <BatchItem>
0274      <Operation type="Enumeration" value="Destroy"/>
0275      <ResultStatus type="Enumeration" value="Success"/>
0276      <ResponsePayload>
0277        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_0"/>
0278      </ResponsePayload>
0279    </BatchItem>
0280  </ResponseMessage>
```

```
          # TIME 6
0281  <RequestMessage>
0282    <RequestHeader>
0283      <ProtocolVersion>
0284        <ProtocolVersionMajor type="Integer" value="1"/>
0285        <ProtocolVersionMinor type="Integer" value="2"/>
0286      </ProtocolVersion>
0287      <BatchCount type="Integer" value="1"/>
0288    </RequestHeader>
0289    <BatchItem>
0290      <Operation type="Enumeration" value="Revoke"/>
0291      <RequestPayload>
0292        <UniqueIdentifier type="TextString"
          value="$UNIQUE_IDENTIFIER_1"/>
0293        <RevocationReason>
0294          <RevocationReasonCode type="Enumeration"
          value="Unspecified"/>
```

```
0295        </RevocationReason>
0296      </RequestPayload>
0297    </BatchItem>
0298  </RequestMessage>
```

```
0299  <ResponseMessage>
0300    <ResponseHeader>
0301      <ProtocolVersion>
0302        <ProtocolVersionMajor type="Integer" value="1"/>
0303        <ProtocolVersionMinor type="Integer" value="2"/>
0304      </ProtocolVersion>
0305      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0306      <BatchCount type="Integer" value="1"/>
0307    </ResponseHeader>
0308    <BatchItem>
0309      <Operation type="Enumeration" value="Revoke"/>
0310      <ResultStatus type="Enumeration" value="Success"/>
0311      <ResponsePayload>
0312        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_1"/>
0313      </ResponsePayload>
0314    </BatchItem>
0315  </ResponseMessage>
```

```
      # TIME 7
0316  <RequestMessage>
0317    <RequestHeader>
0318      <ProtocolVersion>
0319        <ProtocolVersionMajor type="Integer" value="1"/>
0320        <ProtocolVersionMinor type="Integer" value="2"/>
0321      </ProtocolVersion>
0322      <BatchCount type="Integer" value="1"/>
0323    </RequestHeader>
0324    <BatchItem>
0325      <Operation type="Enumeration" value="Destroy"/>
0326      <RequestPayload>
0327        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_1"/>
0328      </RequestPayload>
0329    </BatchItem>
0330  </RequestMessage>
```

```
0331  <ResponseMessage>
0332    <ResponseHeader>
0333      <ProtocolVersion>
0334        <ProtocolVersionMajor type="Integer" value="1"/>
0335        <ProtocolVersionMinor type="Integer" value="2"/>
0336      </ProtocolVersion>
0337      <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
0338      <BatchCount type="Integer" value="1"/>
0339    </ResponseHeader>
0340    <BatchItem>
0341      <Operation type="Enumeration" value="Destroy"/>
0342      <ResultStatus type="Enumeration" value="Success"/>
0343      <ResponsePayload>
0344        <UniqueIdentifier type="TextString"
      value="$UNIQUE_IDENTIFIER_1"/>
0345      </ResponsePayload>
0346    </BatchItem>
0347  </ResponseMessage>
```

3.3 Mandatory Test Cases KMIP v1.2 - RNG

3.3.1 CS-RNG-M-1-12 - RNG Retrieve

Retrieve output from an RNG.

```
# TIME 0
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="RNGRetrieve"/>
    <RequestPayload>
      <DataLength type="Integer" value="32"/>
    </RequestPayload>
  </BatchItem>
</RequestMessage>
```

```
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="2013-06-21T22:18:59+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="RNGRetrieve"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <Data type="ByteString"
value="9c0bcd79d775998ddc52457bbbcfce2d4a194b039e20a3adacb63fb6561ba
545"/>
    </ResponsePayload>
  </BatchItem>
</ResponseMessage>
```

3.4 Optional Test Cases KMIP v1.2 - RNG

3.4.1 CS-RNG-O-1-12 - Seed RNG with Server Accept

RNG Seed with server accepting all the provided seeding material

```
# TIME 0
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="2"/>
    </ProtocolVersion>
```

```
0007      <BatchCount type="Integer" value="1"/>
0008    </RequestHeader>
0009    <BatchItem>
0010      <Operation type="Enumeration" value="RNGSeed"/>
0011      <RequestPayload>
0012        <Data type="ByteString"
        value="333c06587706225099a67438f263f8f932f64b860c3a7dbb21bc2bd56685d
        8bc"/>
0013      </RequestPayload>
0014    </BatchItem>
0015  </RequestMessage>
```

```
0016  <ResponseMessage>
0017    <ResponseHeader>
0018      <ProtocolVersion>
0019        <ProtocolVersionMajor type="Integer" value="1"/>
0020        <ProtocolVersionMinor type="Integer" value="2"/>
0021      </ProtocolVersion>
0022      <TimeStamp type="DateTime" value="2013-06-21T22:58:37+00:00"/>
0023      <BatchCount type="Integer" value="1"/>
0024    </ResponseHeader>
0025    <BatchItem>
0026      <Operation type="Enumeration" value="RNGSeed"/>
0027      <ResultStatus type="Enumeration" value="Success"/>
0028      <ResponsePayload>
0029        <DataLength type="Integer" value="32"/>
0030      </ResponsePayload>
0031    </BatchItem>
0032  </ResponseMessage>
```

219

220 3.4.2 CS-RNG-O-2-12 - Seed RNG with Server partial Accept

221 RNG Seed with server accepting the first sixteen bytes of the provided seeding material

```
      # 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="RNGSeed"/>
0011      <RequestPayload>
0012        <Data type="ByteString"
        value="333c06587706225099a67438f263f8f932f64b860c3a7dbb21bc2bd56685d
        8bc"/>
0013      </RequestPayload>
0014    </BatchItem>
0015  </RequestMessage>
```

```
0016  <ResponseMessage>
0017    <ResponseHeader>
0018      <ProtocolVersion>
0019        <ProtocolVersionMajor type="Integer" value="1"/>
0020        <ProtocolVersionMinor type="Integer" value="2"/>
0021      </ProtocolVersion>
```

```
0022      <TimeStamp type="DateTime" value="2013-06-21T22:59:30+00:00"/>
0023      <BatchCount type="Integer" value="1"/>
0024    </ResponseHeader>
0025    <BatchItem>
0026      <Operation type="Enumeration" value="RNGSeed"/>
0027      <ResultStatus type="Enumeration" value="Success"/>
0028      <ResponsePayload>
0029        <DataLength type="Integer" value="16"/>
0030      </ResponsePayload>
0031    </BatchItem>
0032  </ResponseMessage>
```

222

223 3.4.3 CS-RNG-O-3-12 - Seed RNG with Server Ignore

224 RNG Seed with server ignoring the provided seeding material

```
      # 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="RNGSeed"/>
0011      <RequestPayload>
0012        <Data type="ByteString"
      value="333c06587706225099a67438f263f8f932f64b860c3a7dbb21bc2bd56685d
      8bc"/>
0013      </RequestPayload>
0014    </BatchItem>
0015  </RequestMessage>
```

```
0016  <ResponseMessage>
0017    <ResponseHeader>
0018      <ProtocolVersion>
0019        <ProtocolVersionMajor type="Integer" value="1"/>
0020        <ProtocolVersionMinor type="Integer" value="2"/>
0021      </ProtocolVersion>
0022      <TimeStamp type="DateTime" value="2013-06-21T22:57:22+00:00"/>
0023      <BatchCount type="Integer" value="1"/>
0024    </ResponseHeader>
0025    <BatchItem>
0026      <Operation type="Enumeration" value="RNGSeed"/>
0027      <ResultStatus type="Enumeration" value="Success"/>
0028      <ResponsePayload>
0029        <DataLength type="Integer" value="0"/>
0030      </ResponsePayload>
0031    </BatchItem>
0032  </ResponseMessage>
```

225

226 3.4.4 CS-RNG-O-4-12 - Seed RNG with Server Deny

227 RNG Seed with server denying the operation

```
        # 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="RNGSeed"/>
0011        <RequestPayload>
0012          <Data type="ByteString"
          value="333c06587706225099a67438f263f8f932f64b860c3a7dbb21bc2bd56685d
          8bc"/>
0013        </RequestPayload>
0014      </BatchItem>
0015    </RequestMessage>
```

```
0016    <ResponseMessage>
0017      <ResponseHeader>
0018        <ProtocolVersion>
0019          <ProtocolVersionMajor type="Integer" value="1"/>
0020          <ProtocolVersionMinor type="Integer" value="2"/>
0021        </ProtocolVersion>
0022        <TimeStamp type="DateTime" value="2013-06-21T23:01:47+00:00"/>
0023        <BatchCount type="Integer" value="1"/>
0024      </ResponseHeader>
0025      <BatchItem>
0026        <Operation type="Enumeration" value="RNGSeed"/>
0027        <ResultStatus type="Enumeration" value="OperationFailed"/>
0028        <ResultReason type="Enumeration" value="PermissionDenied"/>
0029        <ResultMessage type="TextString" value="DENIED"/>
0030      </BatchItem>
0031    </ResponseMessage>
```

228

4 Conformance

4.1 Basic Cryptographic Client KMIP v1.2 Profile Conformance

KMIP client implementations conformant to this profile:

1. SHALL support the Basic Cryptographic Client Profile conditions (2.1) and;
2. SHALL support at least one of the Mandatory Test Cases KMIP v1.2 - Basic (3.1).

4.2 Basic Cryptographic Server KMIP v1.2 Profile Conformance

KMIP server implementations conformant to this profile:

1. SHALL support the Basic Cryptographic Server Profile conditions (2.2) and;
2. SHALL support all the Mandatory Test Cases KMIP v1.2 - Basic (3.1).

4.3 Advanced Cryptographic Client KMIP v1.2 Profile Conformance

KMIP client implementations conformant to this profile:

1. SHALL support the Advanced Cryptographic Client Profile conditions (2.3) and;
2. SHALL support at least one of the Mandatory Test Cases KMIP v1.2 - Advanced (3.2).

4.4 Advanced Cryptographic Server KMIP v1.2 Profile Conformance

KMIP server implementations conformant to this profile:

1. SHALL support the Advanced Cryptographic Server Profile conditions (2.4) and;
2. SHALL support all the Mandatory Test Cases KMIP v1.2 - Advanced (3.2).

4.5 RNG Cryptographic Client KMIP v1.2 Profile Conformance

KMIP client implementations conformant to this profile:

1. SHALL support the RNG Cryptographic Client Profile conditions (2.5) and;
2. SHALL support at least one of the Mandatory Test Cases KMIP v1.2 - RNG (3.3).

4.6 RNG Cryptographic Server KMIP v1.2 Profile Conformance

KMIP client implementations conformant to this profile:

1. SHALL support the RNG Cryptographic Server Profile conditions (2.6) and;
2. SHALL support all the Mandatory Test Cases KMIP v1.2 - RNG (3.3).

4.7 Permitted Test Case Variations

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

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

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

4.7.1 Variable Items

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

1. UniqueIdentifier
2. PrivateKeyUniqueIdentifier
3. PublicKeyUniqueIdentifier
4. UniqueBatchItemIdentifier
5. AsynchronousCorrelationValue
6. TimeStamp
7. KeyValue / KeyMaterial including:
    a. key material content returned for managed cryptographic objects which are generated by the server
    b. wrapped versions of keys where the wrapping key is dynamic or the wrapping contains variable output for each wrap operation
8. For response containing the output of cryptographic operation in Data / SignatureData/ MACData / IVCounterNonce where:
    a. the managed object is generated by the server; or
    b. the operation inherently contains variable output
9. For the following DateTime attributes where the value is not specified in the request as a fixed DateTime value:
    a. ActivationDate
    b. ArchiveDate
    c. CompromiseDate
    d. CompromiseOccurrenceDate
    e. DeactivationDate
    f. DestroyDate
    g. InitialDate
    h. LastChangeDate
    i. ProtectStartDate
    j. ProcessStopDate
    k. ValidityDate
    l. OriginalCreationDate
10. LinkedObjectIdentifier
11. DigestValue
    a. For those managed cryptographic objects which are dynamically generated
12. KeyFormatType
    a. The key format type selected by the server when it creates managed objects
13. Digest
    a. The HashingAlgorithm selected by the server when it calculates the digest for a managed object for which it has access to the key material
    b. The Digest Value
14. Extensions reported in Query for ExtensionList and ExtensionMap
15. Application Namespaces reported in Query
16. Object Types reported in Query other than those noted as required in this profile
17. Operation Types reported in Query other than those noted as required in this profile (or any referenced profile documents)
18. For TextString attribute values containing test identifiers:

306 a. Additional vendor or application prefixes
307 19. Additional attributes beyond those noted in the response
308
309 An implementation conformant to this Profile MAY allow the following response variations:
310 20. Object Group values – May or may not return one or more Object Group values not included in
311 the requests
312 21. y-CustomAttributes – May or may not include additional server-specific associated attributes not
313 included in requests
314 22. Message Extensions – May or may not include additional (non-critical) vendor extensions
315 23. TemplateAttribute – May or may not be included in responses where the Template Attribute
316 response is noted as optional in [KMIP-SPEC-1_2]
317 24. AttributeIndex – May or may not include Attribute Index value where the Attribute Index value is 0
318 for Protocol Versions 1.1 and above.
319 25. ResultMessage – May or may not be included in responses and the value (if included) may vary
320 from the text contained within the test case.
321 26. The list of Protocol Versions returned in a DiscoverVersion response may include additional
322 protocol versions if the request has not specified a list of client supported Protocol Versions.
323 27. VendorIdentification - The value (if included) may vary from the text contained within the test
324 case.

325 ### 4.7.2 Variable behavior

326 An implementation conformant to this Profile SHALL allow variation of the following behavior:
327 1. A test MAY omit the clean-up requests and responses (containing Revoke and/or Destroy) at the
328 end of the test provided there is a separate mechanism to remove the created objects during
329 testing.
330 2. A test MAY omit the test identifiers if the client is unable to include them in requests. This
331 includes the following attributes:
332 a. Name; and
333 b. x-ID
334 3. A test MAY perform requests with multiple batch items or as multiple requests with a single batch
335 item provided the sequence of operations are equivalent
336 4. A request MAY contain an optional *Authentication* [KMIP_SPEC] structure within each request
337

Appendix A. Acknowledgments

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

Participants:

Hal Aldridge, Sypris Electronics
Mike Allen, Symantec
Gordon Arnold, IBM
Todd Arnold, IBM
Richard Austin, Hewlett-Packard
Lars Bagnert, PrimeKey
Elaine Barker, NIST
Peter Bartok, Venafi, Inc.
Tom Benjamin, IBM
Anthony Berglas, Cryptsoft
Mathias Björkqvist, IBM
Kevin Bocket, Venafi
Anne Bolgert, IBM
Alan Brown, Thales e-Security
Tim Bruce, CA Technologies
Chris Burchett, Credant Technologies, Inc.
Kelley Burgin, National Security Agency
Robert Burns, Thales e-Security
Chuck Castleton, Venafi
Kenli Chong, QuintessenceLabs
John Clark, Hewlett-Packard
Tom Clifford, Symantec Corp.
Doron Cohen, SafeNet, Inc
Tony Cox, Cryptsoft
Russell Dietz, SafeNet, Inc
Graydon Dodson, Lexmark International Inc.
Vinod Duggirala, EMC Corporation
Chris Dunn, SafeNet, Inc.
Michael Duren, Sypris Electronics
James Dzierzanowski, American Express CCoE
Faisal Faruqui, Thales e-Security
Stan Feather, Hewlett-Packard
David Finkelstein, Symantec Corp.
James Fitzgerald, SafeNet, Inc.
Indra Fitzgerald, Hewlett-Packard
Judith Furlong, EMC Corporation
Susan Gleeson, Oracle
Robert Griffin, EMC Corporation
Paul Grojean, Individual
Robert Haas, IBM
Thomas Hardjono, M.I.T.
ChengDong He, Huawei Technologies Co., Ltd.
Steve He, Vormetric
Kurt Heberlein, Hewlett-Packard
Larry Hofer, Emulex Corporation
Maryann Hondo, IBM
Walt Hubis, NetApp
Tim Hudson, Cryptsoft
Jonas Iggbom, Venafi, Inc.

Sitaram Inguva, American Express CCoE
Jay Jacobs, Target Corporation
Glen Jaquette, IBM
Mahadev Karadiguddi, NetApp
Greg Kazmierczak, Wave Systems Corp.
Marc Kenig, SafeNet, Inc.
Mark Knight, Thales e-Security
Kathy Kriese, Symantec Corporation
Mark Lambiase, SecureAuth
John Leiseboer, Quintenssence Labs
Hal Lockhart, Oracle Corporation
Robert Lockhart, Thales e-Security
Anne Luk, Cryptsoft
Sairam Manidi, Freescale
Luther Martin, Voltage Security
Neil McEvoy, iFOSSF
Marina Milshtein, Individual
Dale Moberg, Axway Software
Jishnu Mukeri, Hewlett-Packard
Bryan Olson, Hewlett-Packard
John Peck, IBM
Rob Philpott, EMC Corporation
Denis Pochuev, SafeNet, Inc.
Reid Poole, Venafi, Inc.
Ajai Puri, SafeNet, Inc.
Saravanan Ramalingam, Thales e-Security
Peter Reed, SafeNet, Inc.
Bruce Rich, IBM
Christina Richards, American Express CCoE
Warren Robbins, Dell
Peter Robinson, EMC Corporation
Scott Rotondo, Oracle
Saikat Saha, SafeNet, Inc.
Anil Saldhana, Red Hat
Subhash Sankuratripati, NetApp
Boris Schumperli, Cryptomathic
Greg Singh, QuintessenceLabs
David Smith, Venafi, Inc
Brian Spector, Certivox
Terence Spies, Voltage Security
Deborah Steckroth, RouteOne LLC
Michael Stevens, QuintessenceLabs
Marcus Streets, Thales e-Security
Satish Sundar, IBM
Kiran Thota, VMware
Somanchi Trinath, Freescale Semiconductor, Inc.
Nathan Turajski, Thales e-Security
Sean Turner, IECA, Inc.
Paul Turner, Venafi, Inc.
Rod Wideman, Quantum Corporation
Steven Wierenga, Hewlett-Packard
Jin Wong, QuintessenceLabs
Sameer Yami, Thales e-Security
Peter Yee, EMC Corporation
Krishna Yellepeddy, IBM
Catherine Ying, SafeNet, Inc.
Tatu Ylonen, SSH Communications Security (Tectia Corp)

Michael Yoder, Vormetric. Inc.
Magda Zdunkiewicz, Cryptsoft
Peter Zelechoski, Election Systems & Software

Appendix B. KMIP Specification Cross Reference

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

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

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

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

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

448

Appendix C. Revision History

Revision	Date	Editor	Changes Made
wd01	27-June-2013	Tim Hudson	Updated conformance wording style. Updated test case style. Included test cases for 1.2. Applied new OASIS template.
wd02	5-July-2013	Tim Hudson	Updated based on review feedback from John Leiseboer. Expanded test cases to include additional modes. Corrected typographical errors.
wd03	10-July-2013	Tim Hudson	Additional test cases added also based on further review feedback from John Leiseboer. Corrected missed section reference in advanced cryptographic conformance clauses. Corrected error handling for CBC examples with missing IV/Counter/Nonce values.
wd04	6-August-2013	Tim Hudson	Updated to include Permitted Test Case Variations and updated Test Cases based on July 2013 Interop
wd05	10-August-2013	Tim Hudson	Updated Permitted Test Case Variations
wd05a	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