Key Management Interoperability Protocol Use Cases Version 1.0

Committee Specification 01

15 June 2010

Specification URIs:
This Version:
http://docs.oasis-open.org/kmip/usecases/v1.0/cs01/kmip-usecases-1.0-cs-01.html
http://docs.oasis-open.org/kmip/usecases/v1.0/cs01/kmip-usecases-1.0-cs-01.doc (Authoritative)
http://docs.oasis-open.org/kmip/usecases/v1.0/cs01/kmip-usecases-1.0-cs-01.pdf

Previous Version:
http://docs.oasis-open.org/kmip/usecases/v1.0/cd11/kmip-usecases-1.0-cd-11.html
http://docs.oasis-open.org/kmip/usecases/v1.0/cd11/kmip-usecases-1.0-cd-11.doc (Authoritative)
http://docs.oasis-open.org/kmip/usecases/v1.0/cd11/kmip-usecases-1.0-cd-11.pdf

Latest Version:
http://docs.oasis-open.org/kmip/usecases/v1.0/kmip-usecases-1.0.html
http://docs.oasis-open.org/kmip/usecases/v1.0/kmip-usecases-1.0.doc
http://docs.oasis-open.org/kmip/usecases/v1.0/kmip-usecases-1.0.pdf

Technical Committee:
OASIS Key Management Interoperability Protocol (KMIP) TC

Chair(s):
Robert Griffin, EMC Corporation <robert.griffin@rsa.com>
Subhash Sankuratripati, NetApp <Subhash.Sankuratripati@netapp.com>

Editor(s):
Mathias Björkqvist, IBM <mbj@zurich.ibm.com>
René Pawlitzek, IBM <rpa@zurich.ibm.com>

Related work:
This specification replaces or supersedes:

- None

This specification is related to:

- Key Management Interoperability Protocol Specification Version 1.0
- Key Management Interoperability Protocol Profiles Version 1.0
- Key Management Interoperability Protocol Usage Guide Version 1.0

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

Status:
This document was last revised or approved by the Key Management Interoperability Protocol TC on the above date. The level of approval is also listed above. Check the “Latest Version” or “Latest Approved Version” location noted above for possible later revisions of this document.

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

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

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/kmip/.

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 names "OASIS", “KMIP” are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

1 Introduction

The purpose of this document is to describe use-cases to demonstrate the Key Management Interoperability Protocol (KMIP) **[KMIP-Spec]**. The use-cases indicate if all concepts within the protocol are sound and if the protocol is usable when implementing typical scenarios in real life. These use-cases are not intended to fully test an implementation of KMIP. Thus, the use-cases do not contain typical Quality Assurance scenarios which would stress an implementation. The use-cases are based on v1.0 of the protocol.

The use-cases define a number of client-to-server request-response pairs for a number of operations. For each request-response message pair the operation is stated, along with the relevant parameters needed for the request or response message. This is followed by two different illustrations of the messages: first, a human-readable construction which shows the fields tags, types and values, followed by the TTLV-encoding of the message. These are included to facilitate the implementation of the message creation and parsing functionality. The use-cases show one possible way to construct the messages, and the messages shown are not necessarily the only correct constructions (e.g. it is possible to omit the attribute index if it is zero). Also note that many values change dynamically when running the use-cases (the server-generated timestamps, Unique Identifiers and key material in responses, as well as Batch Item ID values in client-generated requests).

In many situations in the use cases defined in this document, the server behavior depends on the server's policy. The illustrated message exchanges and their contents are not the only possible variants (see **[KMIP-Spec]**). E.g., the server response messages shown in this document correspond to a server policy of completely destroying a managed object, along with all of its attributes, when receiving a Destroy request.

Multiple use cases describe several clients operating on the same managed object(s). For this to work, the clients SHALL have authenticated themselves to the server using the same credentials (see **[KMIP-Prof]**). Alternatively, the server policy applied to the relevant managed object(s) SHALL be such that the clients all have access to the managed object(s) in question.

1.1 Normative References

[KMIP-Spec] OASIS Committee Specification 01, Key Management Interoperability Protocol Specification Version 1.0, June 2010, http://docs.oasis-open.org/kmip/spec/v1.0/cs01/kmip-spec-1.0-cs-01.doc

[KMIP-Prof] OASIS Committee Specification 01, Key Management Interoperability Protocol Profiles Version 1.0, June 2010, http://docs.oasis-open.org/kmip/profiles/v1.0/cs01/kmip-profiles-1.0-cs-01.doc

2 Message exchange

The message exchange between clients and the server to test the following use-case scenarios is performed with TTLV encoding over the TLS/SSL transport as defined in **[KMIP-Spec]** and **[KMIP-Prof]**.

3 Centralized Management

3.1 Basic functionality

These use-cases test the basic features of KMIP including key creation, template and secret data registration, attribute functionality, access methods, and batch operation.

3.1.1 Use-case: Create / Destroy

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

Time	Request/Response messages
0	Create (symmetric key) In: objectType='00000002' (Symmetric Key), attributes={ CryptographicAlgorithm='00000003' (AES), CryptographicLength='128', CryptographicUsageMask='0000000C' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt) 420078010000012042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000004 2 974686D0042000B050000000400000003000000004200080100000030420 00A07000000144372797074 6F6772617068696320 4C656E6774680 Out: objectType='00000002', uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C2 (Thu Nov 12 11:47:30 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

	Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fc8833de-70d2-4ece-b063-fede3a3c59fe 42007B01000000C042007A01000000484200690100000020420 06A0200000004000000010000000042006B020000000400000000000000004283333646 52D373064322D346563652D623036332D666564653361336335396665000000000
1	Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fc8833de-70d2-4ece-b063-fede3a3c59fe 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C3 (Thu Nov 12 11:47:31 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fc8833de-70d2-4ece-b063-fede3a3c59fe 42007B01000000B042007A01000000484200690100000020420 06A0200000004000000010000000042006B020000000400000000000000004223036332D666564653361336335396665000000000

87

88

89 3.1.2 Use-case: Register / Create / Get attributes / Destroy

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

93

Time	Request/Response messages
0	Register (template) In: objectType='00000007', TemplateAttribute=empty, Template={ ObjectGroup='Group1', ApplicationSpecificInformation='s

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000006 (Template)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: null
      Tag: Template (0x420090), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Application Specific Information
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Application Namespace (0x420003), Type: Text String (0x07), Data: ssl
            Tag: Application Data (0x420002), Type: Text String (0x07), Data: www.example.com
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-Purpose
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: demonstration
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: Template1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007801000001C84200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
0000000042000B070000000647726F757031000042000801000000584200A0700000020417070 6C69636174696F6E20537065636969666932
034A6F650000000000420008010000003042000A0700000009782D507572706F7365000000000000000042000B070000000D64656D6F6E737472
```

Out: uuidTemplate

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C4 (Thu Nov 12 11:47:32 CET 2009)
```

	Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a6ebbb6f-4c54-4bbb-ad29-be6bad4ecad5 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004216432392D6265366261643465636161643500000000
1	Create (symmetric key using template) In: objectType='00000002', template={ NameValue='Template1', NameType='00000001' }, attributes={ CryptographicAlgori Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Name (0x420053), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Template1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt) 42007801000001504200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004250000000400000001000000004200080100000003042000A07000000174372797074 6F6772617068696320416C676F726974686D0042000B0506B42000B020000000400000000C00000000 Out: objectType='00000002', uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C5 (Thu Nov 12 11:47:33 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

	Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-2fa6ea1d747a 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004242 1303631342D643862352D343666392D386431372D326661366561316437343761000000000
2	Get attributes In: uuidKey, attributeNames={'ObjectGroup', 'ApplicationSpecificInformation', 'ContactInformation', 'x-Purpose'} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-2fa6ea1d747a Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Application Specific Information Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-Purpose 420078010000010842007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000004242 563742047726F7570000000000042000A0700000020417070 6C69636174696F6E20537065636966696320496E666F726D6174696F6E42000A070 Out: uuidKey, attributes={ ObjectGroup='Group1', ApplicationSpecificInformation='ssl, www.example.com', ContactInformati Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C6 (Thu Nov 12 11:47:34 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-2fa6ea1d747a Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1 Tag: Attribute (0x420008), Type: Structure (0x01), Data:

	Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Application Specific Information Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Application Namespace (0x420003), Type: Text String (0x07), Data: ssl Tag: Application Data (0x420002), Type: Text String (0x07), Data: www.example.com Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-Purpose Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: demonstration 42007B01000001B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042 86431372D32666136656131643734376100000000420008010000002842000A070000000C4F626A6563742047726F757000000000042000B070 00420008010000003042000A0700000013436F6E7461637420496E666F726D6174696F6E000000000042000B07000000034A6F650000000000
3	Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-2fa6ea1d747a 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C6 (Thu Nov 12 11:47:34 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-2fa6ea1d747a 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042 86431372D3266613665613164373437610000000
4	Destroy (template)

	In: uuidTemplate
	
	`Tag: Request Message (0x420078), Type: Structure (0x01), Data:`
	`  Tag: Request Header (0x420077), Type: Structure (0x01), Data:`
	`  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)`
	`  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:`
	`  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)`
	`  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:`
	`  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a6ebbb6f-4c54-4bbb-ad29-be6bad4ecad5`
	
	`42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042`
	
	Out: uuidTemplate
	
	`Tag: Response Message (0x42007B), Type: Structure (0x01), Data:`
	`  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:`
	`  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)`
	`  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C6 (Thu Nov 12 11:47:34 CET 2009)`
	`  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:`
	`  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)`
	`  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)`
	`  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:`
	`  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a6ebbb6f-4c54-4bbb-ad29-be6bad4ecad5`
	
	`42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042`
	`16432392D626536626164346563616435000000000`

3.1.3 Use-case: Create / Locate / Get / Destroy

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

Time	Request/Response messages
0	Create (symmetric key) In: objectType = ‘00000002’, attributes={ Name={ NameValue=‘Key1’, NameType=’00000001’ }, CryptographicAlgorithm=’D `Tag: Request Message (0x420078), Type: Structure (0x01), Data:`

```
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (3DES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x000000A8 (168)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe

42007801000001984200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
7000000044B65793100000000420054050000000400000001000000042000801000000304 2000A0700000017437279707 46F6772617068696
726170686963205573616765204D61736B42000B020000000400000000C000000042000801000000304 2000A0700000013436F6E746163742
```

Out: objectType = ‘00000002’, uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C7 (Thu Nov 12 11:47:35 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890

42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
```

	2386561352D326233312D343134352D626366322D333664303735366433383933000000000
1	Locate (symmetric key) In: attributes={ objectType = '00000002', Name={ Name='Key1', NameType='00000001'} } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007801000000D042007701000000384200690100000020420 06A0200000004000000010000000042006B020000000400000000000000004270000000044E616D650000000042000B01000000204200550700000004 4B65793100000000420054050000000400000001000000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C8 (Thu Nov 12 11:47:36 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890 42007B01000000B042007A01000000484200690100000020420 06A0200000004000000010000000042006B020000000400000000000000004270000000026366322D333664303735366433383933000000000
2	Get (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data:

```
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890
```

```
42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
```

Out: objectType = '00000002', uuidKey, symmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C8 (Thu Nov 12 11:47:36 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data: C8E51523F73D6EE9F40EAB7CD06825499D8C0BD
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000002 (3DES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x000000A8 (168)
```

```
42007B01000001284200 7A01000000484200690100000020 42006A020000000400000001000000042006B020000000400000000000000042
2386561352D326233312D343134352D626366322D333664303735366433383930000000000042008F010000006042004001000000584200420500
```

3	Destroy (symmetric key) In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
```

	Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000000420 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C8 (Thu Nov 12 11:47:36 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000000420 26366322D333664303735366433383930000000000
4	Locate In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Unique Identifier Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890 42007801000000B84200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000000420 3312D343134352D626366322D333664303735366433383930000000000 Out: <empty response payload> Tag: Response Message (0x420078), Type: Structure (0x01), Data: Tag: Response Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420067), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x42008F), Type: Date-Time (0x09), Data: 0x000000004AC07323 (Mon Sep 28 10:26:11 CEST 2009)

	Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420079), Type: Structure (0x01), Data: null 42007B01000000804200 7A01000000484200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000004 2

102

103

104 3.1.4 Use-case: Dual client use-case, ID Placeholder linked Locate & Get batch

105 This use-case has two clients performing operations on the same key. The first client initially registers a
106 template and creates a symmetric key using that template. The second client then does a batched Locate
107 and Get using the ID Placeholder to retrieve the key. The second client thereafter performs a number of
108 operations on the key (Get Attribute List, Get Attribute, Add Attribute, Modify Attribute and Delete
109 Attribute), before the first client finally destroys the key and the template. The first client also tries to Get
110 the key and the template after they have been destroyed, but the Get operation fails in both cases.

111

112 This use-case demonstrates the fact that it is possible for two clients to cooperate and use the same
113 managed object while only having knowledge of a single pre-agreed Name attribute value and without
114 having to share any other information.

115

Time	Request/Response messages
0	Client A: Register (template) In: objectType='00000007', TemplateAttribute=empty, Template={ CryptographicAlgorithm='AES', CryptographicLength='12 Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000006 (Template) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: null Tag: Template (0x420090), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name

	Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Template1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007801000001384200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004296320416C676F726974686D0042000B0500000004000000030000000042000801000000 3042000A07000000144372797074 6F6772617068696 Out: uuidTemplate Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED21 (Thu Nov 12 12:10:25 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 45d8629a-9ad1-41b3-9d09-941f2a595da3 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004296430392D393431663261353935646133000000 00
1	Client A: Create (symmetric key using template) In: objectType='00000002', template={ NameValue= 'Template1', NameType='00000001' }, attributes={ Name={ Name='Ke Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Name (0x420053), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Template1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) Tag: Attribute (0x420008), Type: Structure (0x01), Data:

```
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
        Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Foo
```

42007801000001584200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000000042
50000000400000001000000004200080100000003842000A07000000044E616D650000000042000B010000002042005507000000044B6579310
74696F6E00000000000042000B0700000003466F6F0000000000

Out: objectType='00000002', uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED23 (Thu Nov 12 12:10:27 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
```

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000000042
3653833652D356237612D343836352D393634612D38643163336262663961653300000000

2

Client B:

Locate and Get (symmetric key by name)

In (header): batchOrderOption='TRUE'

In: attributes={ objectType = '00000002', Name={ Name='Key1', NameType='00000001'} }

In: <empty Get payload>

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 0E9E1875336E415E
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
```

```
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: CFEF21DDDF1CF5E3
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data: null
```

```
42007801000001204200770100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004200
0000000042000B050000000400000002000000004200080100000038420 00A07000000044E616D650000000042000B01000000204200550700
```

Out: uuidKey

Out: objectType='00000002', uuidKey, symmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED24 (Thu Nov 12 12:10:28 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 0E9E1875336E415E
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: CFEF21DDDF1CF5E3
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 755D03C639648FB5828D5F1CC9FE9B57
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
```

```
42007B01000001A042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004200
3653833652D356237612D343836352D393634612D386431633362626639616533000000004200 0F01000000D842005C050000000400000000
0042008F010000005842004001000000504200420500000000400000001000000004200450100000018420043080000000755D03C639648FB5
```

3	Client B: Get attribute list

	In: uuidKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
	
	42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004 2
	
	Out: uuidKey, attributes={ * }
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED24 (Thu Nov 12 12:10:28 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digest
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Initial Date
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Unique Identifier
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Last Change Date
	
	42007B01000001C842007A01000000484200690100000020420 6A020000000400000001000000042006B020000000400000000000000042
	93634612D3864316333626266396165330000000042000A0700000014437279707 46F6772617068696320 4C656E6774680000000042000A070
	65720000000000000042000A07000000044E616D650000000042000A0700000018437279707 46F6772617068696320557361676520 4D61736

4	Client B: Get attributes In: uuidKey, attributeNames={‘Name’, ‘ContactInformation’}

	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
	
	42007801000000C0420077010000003842006901000000 2042006A020000000400000001000000042006B020000000400000000000000004250000000042000A0700000013436F6E7461637420496E666F726D6174696F6E0000000000
	
	Out: uuidKey, attributes={ Name={ Name='Key1', NameType='00000001' }, ContactInformation='Foo' }
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED24 (Thu Nov 12 12:10:28 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
	  Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
	  Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
	  Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
	  Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Foo
	
	42007B01000001284200 7A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004293634612D3864316333626266396165330000000042000801000000384200 0A07000000044E616D650000000042000B01000000204200550700

5	Client B: Add attribute [batch] In: uuidKey, attribute={ x-attribute1='Value1'} In: uuidKey, attribute={ x-attribute2='Value2' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data:

```
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7A92DDA525EB158A
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value1
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7230F6E4D3BEA249
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value2

42007801000001604200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
3000000004200080100000028420 00A070000000C782D617474726962757465310000000042000B0700000006566 16C756531000042000F010
0C782D617474726962757465320000000042000B070000000656616C7565320000
```

Out: uuidKey, attribute={ x-attribute1='Value1'}

Out: uuidKey, attribute={ x-attribute2='Value2' }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED25 (Thu Nov 12 12:10:29 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7A92DDA525EB158A
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value1
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7230F6E4D3BEA249
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
```

	Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value2 42007B01000001904200 7A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042 3653833652D356237612D343836352D393634612D386431633362626639616533000000004200080100000028420 00A070000000C782D61747 652D356237612D343836352D393634612D386431633362626639616533000000004200080100000028420 00A070000000C782D617474726962
6	Client B: Modify attribute [batch] In: uuidKey, attribute={ x-attribute1='ModifiedValue1' } In: uuidKey, attribute={ x-attribute2='ModifiedValue2' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BA3EA60548ECB699 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 321984E716274A3D Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2 42007801000001704200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042 3000000004200080100000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F6469666964566456616C756 3042000A070000000C782D617474726962757465320000000042000B070000000E4D6F6469666964566456616C7565320000 Out: uuidKey, attribute={ x-ttribute1='ModifiedValue1' } Out: uuidKey, attribute={ x-attribute2='ModifiedValue2' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

	Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED26 (Thu Nov 12 12:10:30 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BA3EA60548ECB699 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 321984E716274A3D Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2 42007B01000001A042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042 3653833652D356237612D343836352D393634612D386431633362626639616533000000004200080100000030420 00A070000000C782D61747 2430613333653833652D356237612D343836352D393634612D386431633362626639616533000000004200080100000030420 00A070000000C
7	Client B: Delete attribute [batch] In: uuidKey, attributeNames={'x-attribute1'} In: uuidKey, attributeNames={'x-attribute2'} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D5C6DF842DAEECD8 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 572D4F0D433DAB10 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 42007801000001304200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042

	30000000042000A070000000C782D617474726962757465310000000042000F010000007042005C050000000400000000F00000000420093080
	
	Out: uuidKey, attributeNames={'x-attribute1'}
	Out: uuidKey, attributeNames={'x-attribute2'}
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED26 (Thu Nov 12 12:10:30 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
	  Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D5C6DF842DAEECD8
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
	  Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
	  Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 572D4F0D433DAB10
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
	  Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2
	
	42007B01000001A042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
	3653833652D356237612D343836352D393634612D3864316333626266396165330000000042000801000000304200 0A070000000C782D61747
	2430613333653833652D356237612D343836352D393634612D3864316333626266396165330000000042000801000000304200 0A070000000C

8	Client A:
	Destroy (symmetric key)
	In: uuidKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

	42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
	
	Out: uuidKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED27 (Thu Nov 12 12:10:31 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
	
	42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
	93634612D386431633362626639616533000000000

9	Client A:
	Get (symmetric key)
	In: uuidKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
	
	42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
	
	Out: Operation Failed, Item Not Found
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED27 (Thu Nov 12 12:10:31 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

	Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed) Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x00000001 (Item Not Found) Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Object does not exist 42007B01000000A842007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004206E6F74206578697374000000
10	Client A: Destroy (template) In: uuidTemplate Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 45d8629a-9ad1-41b3-9d09-941f2a595da3 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004204200770100000038420069010000002042006A020000000400000001000000042006B02000000040000000000000000 Out: uuidTemplate Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED27 (Thu Nov 12 12:10:31 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 45d8629a-9ad1-41b3-9d09-941f2a595da3 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004296430392D393431663261353935646133000000000
11	Client A: Get (template) In: uuidTemplate Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data:

	Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 45d8629a-9ad1-41b3-9d09-941f2a595da3 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042 Out: Operation Failed, Item Not Found Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED27 (Thu Nov 12 12:10:31 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Failed) Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x00000001 (Item Not Found) Tag: Result Message (0x42007D), Type: Text String (0x07), Data: No Cryptographic Object found with given Uniqu 42007B01000000D042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042 170686963204F626A65637420666F756E64207769746820676976656E20556E697175652049646564657200000000000000

116

117 **3.1.5** Use-case: Register / Destroy Secret Data

118 In this use-case the client issues a Register request containing a Secret Data object, whereby the server
119 registers the object and returns the Unique Identifier. To clean up, the client then performs a Destroy
120 operation to destroy the object.

121

Time	Request/Response messages
0	Register (secret data) In: objectType='00000007' (Secret Data), attributes={ CryptographicUsageMask='00000002' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)

	Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000007 (Secret Data) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000002 (Verify) Tag: Secret Data (0x420085), Type: Structure (0x01), Data: Tag: Secret Data Type (0x420086), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000002 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 536563726574506173737767264 42007801000001004200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004204D61736B42000B020000000400000002000000004200850100000048420086050000000400000001000000004200400100000030420042050 Out: uuidObject Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B7924D1 (Mon Feb 15 11:41:21 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 39622cc2-e5d4-4da9-9f10-3bdf64b0e760 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004296631302D33626466363462306537363000000000
1	Destroy (secret data) In: uuidObject Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 39622cc2-e5d4-4da9-9f10-3bdf64b0e760 42007801000000904200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004200

	Out: uuidKey
	
	`Tag: Response Message (0x42007B), Type: Structure (0x01), Data:`
	`  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:`
	`    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)`
	`    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B7924D1 (Mon Feb 15 11:41:21 CET 2010)`
	`    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:`
	`    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)`
	`    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)`
	`    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:`
	`      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 39622cc2-e5d4-4da9-9f10-3bdf64b0e760`
	
	42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000000042
	96631302D33626466363462306537363000000000

3.2 Use-case: Asynchronous Locate

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

This use-case shows the use of two clients with the same assumptions as in the use-case described in Section 3.1.4 Since the client is unable to force the server to respond asynchronously, it is possible for a server to respond synchronously to the requests issued at times 1 and 4, in which case the expected response are the ones shown at times 2 and 5, respectively. In the case of the server not responding asynchronously to the Locate requests, the client is permitted to skip the requests illustrated at time 7 and 8.

Time	Client A

0	Client A:
	Create (symmetric key)
	In: objectType = ‘00000002’, attributes={ CryptographicAlgorithm=’AES’, CryptographicLength=’128’, Name={ NameValue=‘
	
	`Tag: Request Message (0x420078), Type: Structure (0x01), Data:`
	`  Tag: Request Header (0x420077), Type: Structure (0x01), Data:`
	`    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)`
	`    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)`

```
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1

42007801000001904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
974686D0042000B0500000004000000030000000042000801000000 3042000A07000000144372797074 6F67726170686963204C656E6774680
726170686963205573616765204D61736B42000B020000000400000004000000004200080100000028 42000A070000000C4F626A6563742047

Out: objectType = ‘00000002’, uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED28 (Thu Nov 12 12:10:32 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca

42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
0653662332D386564632D346666622D613838652D653136343533396462636361000000000
```

1	Client B: Locate (symmetric key by name) In: asynchronousIndicator=’TRUE’, attributes={ objectType = ‘00000002’, Name={ Name=‘Key1’, NameType=’00000001’} }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007801000000E042007701000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000004220
0000000042000801000000384200 0A07000000044E616D650000000042000B01000000204200550700000044B65793100000000420054050
```

Out: asyncCorrValue1

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED28 (Thu Nov 12 12:10:32 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Pending)
    Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 130BC369AF005A7F

42007B01000000 8842007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004220
```

2 Client B:

Poll*

In: asyncCorrValue1

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
```

	Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 130BC369AF005A7F 42007801000000704200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004 2 Out: uuidKey1 Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED28 (Thu Nov 12 12:10:32 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004 2 13838652D653136343533396462636361000000000
3	Client B: Get (symmetric key) In: uuidKey1 Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004 2 Out: objectType = ‘00000002’, uuidKey1, symmetricKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

```
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data: BEF01F82DFB4682A01C2A08413834AAB
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

42007B010000012042007A0100000048420069010000002042006A02000000040000000100000000420
0653662332D386564632D346666622D613838652D653136343533396462636361000000042008F01000
```

4 Client B:

Locate (symmetric key by group)

In: asynchronousIndicator='TRUE', attributes={ objectType = '00000002', ObjectGroup='Group1' }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1

4200780100000D042007701000000484200690100000020420 06A02000000040000000100000000420
20000000042000801000000284200 0A070000000C4F626A6563742047726F757000000000042000B07000000647726F7570310000
```

Out: asyncCorrValue2

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
```

	Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Pending) Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 48D43C207CD1FB3A 42007B0100000008842007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
5	Client B: Poll* In: asyncCorrValue2 Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 48D43C207CD1FB3A 42007801000000704200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042 Out: uuidKey2 Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042 13838652D653136343533396462636361000000000
6	Client B: Get (symmetric key) In: uuidKey2

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca
```

```
42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
```

Out: objectType = ‘00000002’, uuidKey2, symmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data: BEF01F82DFB4682A01C2A08413834AAB
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
```

```
42007B01000001204200 7A01000000484200690100000020 42006A020000000400000001000000042006B020000000400000000000000042
0653662332D386564632D346666622D613838652D653136343533396462636361000000000 42008F010000005842004001000000504200420 50
```

7	Client B: Locate (symmetric key by name) In: asynchronousIndicator=’TRUE’, attributes={ objectType = ‘00000002’, Name= { Name=‘Key1’, NameType=’00000001’ } }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
```

```
    Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
```


42007801000000E042007701000000484200690100000020420006A020000000400000001000000000420006B02000000040000000000000000042
200000000420008010000003842000A07000000044E616D650000000042000B010000002042005507000000044B65793100000000420054050

Out: asyncCorrValue5

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Pending)
    Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 4D6BBFC35FE57FBA
```


42007B010000008842007A010000004842006901000000204200 6A020000000400000001000000000420006B02000000040000000000000000042

8 Client B:

Cancel

In: asyncCorrValue5

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000019 (Cancel)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 4D6BBFC35FE57FBA
```


4200780100000070420077010000003842006901000000204200 6A020000000400000001000000000420006B02000000040000000000000000042

Out: asyncCorrValue5, CancelResult='00000001'

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000019 (Cancel)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 4D6BBFC35FE57FBA
      Tag: Cancellation Result (0x420012), Type: Enumeration (0x05), Data: 0x00000001 (Cancelled)

42007B01000000A042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000000421
00000000
```

9

Client A:

Destroy (symmetric key)

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca

420078010000009042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000042
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2A (Thu Nov 12 12:10:34 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
```

	Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004213838652D65313634353339646263636100000000

139 * = executed until response is ready

140

141

142 4 Key life cycle support

143

144 4.1 Use-case: Revoke scenario

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

153

Time	Client
0	Client A: Create (symmetric key) In: objectType = '00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', Name={ NameValue=' Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name

	Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt) 42007801000001604200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042 974686D0042000B0500000004000000030000000042000801000000342000A07000000144372797074 6F67726170686963204C656E6774680 726170686963205573616765204D61736B42000B020000000400000004000000000 Out: objectType = ‘00000002’, uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042 2386238612D303664662D343363302D623732662D326131363136333361646139000000000
1	Client A: Get attribute In: uuidKey, attributeName={‘State’} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 42007801000000A042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000042 465000000

	Out: uuidKey, attribute={ State='00000001' }
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
	  Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000001 (Pre-Active)
	
	42007B01000000D842007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000000420
	23732662D3261313631363333616461390000000042000801000000204200 0A0700000005537461746500000042000B05000000040000000100

2	Client A:
	Activate
	In: uuidKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000012 (Activate)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
	
	420078010000009042007701000000384200690100000020420 6A020000000400000001000000042006B020000000400000000000000004204
	
	Out: uuidKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

	Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000012 (Activate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004223732662D32613136313633336164613900000000
3	Client A: Get attribute In: uuidKey, attributeName={ 'State' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 42007801000000A042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000004223732662D32613136313633336164613900000000 Out: uuidKey, attribute={ State='00000002' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active) 42007B01000000D842007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004223732662D32613136313633336164613900000000420008010000002042000A07000000055374617465000000042000B050000000400000002
4	Client B: Locate (symmetric key by name)

	In: objectType = ‘00000002’, attributes={ Name={ Name=‘Key1’, NameType=’00000001’ } }
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
	  Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
	  Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
	  Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
	  Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
	
	42007801000000D042007701000000384200690100000020420 06A0200000040000000100000000420 06B020000000400000000000000004270000000044E616D650000000042000B0100000020420055070000000044B65793100000000420054050000000400000001000000000
	
	Out: uuidKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
	
	42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000000004223732662D326131363136333361646139000000000

5	Client B:
	Get (symmetric key)
	In: uuidKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

	Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042 Out: objectType = '00000002', uuidKey, symmetricKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: EF7833AB15F5A1EE5874BC0D9BBC4BE7 Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128) 42007B01000001204200 7A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042 2386238612D303664662D343363302D623732662D326131363136333361646139000000000042008F0100000058420040010000005042004205
6	Client B: Revoke (symmetric key as compromised) In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceTime='6' Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9

	Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data: Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000002 (Key Compromise) Tag: Compromise Occurrence Date (0x420021), Type: Date-Time (0x09), Data: 0x0000000000000006 (Thu Jan 01 01: 42007801000000B84200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004250000000400000002000000004200210900000008000000000000006 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004223732662D3261313631363333616461390000000
7	Client B: Get attribute In: uuidKey, attributeName={ ‘State’ } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 42007801000000A042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000004246500000 0 Out: uuidKey, attribute={ State=‘00000004’ } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

```
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2C (Thu Nov 12 12:10:36 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Compromised)

42007B01000000D842007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
23732662D3261313631363333616461390000000042000801000000204200A0700000005537461746500000042000B050000000400000004
```

8

Client A:

Get attribute list

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9

42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
```

Out: uuidKey, attributes = { * }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2C (Thu Nov 12 12:10:36 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
```

	Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Compromise Occurrence Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Compromise Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digest Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Initial Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Revocation Reason Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Unique Identifier Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Last Change Date 42007B01000002204200 7A0100000048420069010000002042006A02000000040000000100000000420 06B020000000400000000000000004223732662D32613136313633336164613900000000042000A0700000014437279707 46F6772617068696320 4C656E6774680000000042000A0700042000A07000000064469676573740000042000A070000000C496E697469616C20446174650000000042000A070000000F4163746976617469 8696320557361676520 4D61736B42000A070000000B4F626A65637420547970650000000000042000A07000000104C617374204368616E67652
9	Client A: Get attributes In: uuidKey, attributeName = { ‘State’ } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 42007801000000A04200770100000038420069010000002042006A02000000040000000100000000420 06B020000000400000000000000004246500000 Out: uuidKey, attribute={ State=‘00000004’ } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2C (Thu Nov 12 12:10:36 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

	Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Compromised) 42007B01000000D842007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042 23732662D3261313631363333616461390000000042000801000000204200 0A070000005537461746500000042000B050000000400000004
10	Client A: Add attribute [batch] In: uuidKey, attribute={ x-attribute1='Value1' } In: uuidKey, attribute={ x-attribute2='Value2' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 9D407FFB45C95672 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value1 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D62107C3158409D8 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value2 42007801000001604200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042 900000000420008010000002842000A070000000C782D617474726962757465310000000042000B070000000656616C756531000042000F010 0C782D617474726962757465320000000042000B070000000656616C7565320000 Out: uuidKey, attribute={ x-attribute1='Value1' } Out: uuidKey, attribute={ x-attribute2='Value2' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2C (Thu Nov 12 12:10:36 CET 2009)

	Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 9D407FFB45C95672 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value1 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D62107C3158409D8 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value2 42007B01000001904200 7A01000000484200690100000020 42006A020000000400000001000000004200 6B020000000400000000000000004 2 2386238612D303664662D343363302D623732662D32613136313633336164613900000000420008010000002842000A070000000C782D61747 612D303664662D343363302D623732662D32613136313633336164613900000000420008010000002842000A070000000C782D617474726962
11	Client A: Modify attribute [batch] In: uuidKey, attribute={ x-attribute1='ModifiedValue1' } In: uuidKey, attribute={ x-attribute2='ModifiedValue2' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 47FB42CCECA3F6EC Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 08019A230A05E9E1 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data:

	Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2 42007801000001704200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042 900000000420008010000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F6469666965645616C756 3042000A070000000C782D6174747269627574653200000000042000B070000000E4D6F64696669656456616C7565320000 Out: uuidKey, attribute={ x-attribute1='ModifiedValue1' } Out: uuidKey, attribute={ x-attribute2='ModifiedValue2' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2D (Thu Nov 12 12:10:37 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 47FB42CCECA3F6EC Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 08019A230A05E9E1 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2 42007B01000001A042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042 2386238612D303664662D343363302D623732662D326131363136333361646139000000004200080100000030420 00A070000000C782D61747 24323164323862386238612D303664662D343363302D623732662D326131363136333361646139000000004200080100000030420 00A070000000C
12	Client A: Delete attribute [batch] In: uuidKey, attributeNames={ 'x-attribute1' } In: uuidKey, attributeNames={ 'x-attribute2' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

```
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3E2C080FA8806057
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 9D55988D43D23B82
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2

42007801000001304200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
90000000042000A070000000C782D617474726962757465310000000042000F010000007042005C050000000400000000F0000000420093080
```

Out: uuidKey, attributeNames={ ‘x-attribute1’ }
Out: uuidKey, attributeNames={ ‘x-attribute2’ }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2D (Thu Nov 12 12:10:37 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3E2C080FA8806057
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 9D55988D43D23B82
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2

42007B01000001A042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
2386238612D303664662D343363302D623732662D326131363136333361646139000000004200080100000030420 00A070000000C782D61747
```

	2432316432386238612D303664662D343363302D623732662D3261313631363333616461390000000042000801000000304200A0700000000
13	Client A: Get (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042 Out: objectType = ‘00000002’, uuidKey, symmetricKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2D (Thu Nov 12 12:10:37 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: EF7833AB15F5A1EE5874BC0D9BBC4BE7 Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128) 42007B01000001204200 7A01000000484200690100000020 42006A020000000400000001000000042006B020000000400000000000000042 2386238612D303664662D343363302D623732662D3261313631363333616461390000000042008F01000000584200400100000050420042050
14	Client A: Destroy (symmetric key) In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
```

```
42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2E (Thu Nov 12 12:10:38 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
```

```
42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
23732662D326131363136333361646139000000000
```

5 Auditing and reporting

5.1 Use-case: Get usage allocation scenario

This use-case tests the usage management functionality of KMIP. A key is created and the Activation Date and Protect Stop Date attributes are set in such a way as to allow the Get Usage Allocation operation to be performed. The value of the Usage Limits attribute is set to 1000 bytes, and two subsequent requests for 500 bytes succeed (one of them also verifying the amount that can be received using the Check operation), while a third fails since the usage allocation has been used up. The key is finally revoked and destroyed. This use-case shows the use of multiple clients with the assumptions regarding the clients being the same as in the use-case described in Section 3.1.4

Time	Client A
0	Client A:

Create (symmetric key)

In: objectType = ‘00000002’, attributes={ CryptographicAlgorithm=’AES’, CryptographicLength=’128’, NameValue={ Name=‘Key1’, NameType=’00000001’ }, CryptographicUsageMask=‘00000004’ }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt)
```

```
42007801000001604200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
974686D0042000B0500000004000000030000000042000801000000304200 0A0700000014437279707 46F67726170686963204C656E6774680
726170686963205573616765204D61736B42000B020000000400000004000000 00
```

Out: objectType = ‘00000002’, uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05A (Thu Mar 11 13:21:46 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
```

	Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d 42007B01000000C042007A01000000484200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000004 2 6656264302D386562612D343036652D626532312D643930353965323962613164000000000
1	Client A: Add attribute [batch] In: uuidKey, attribute={ ActivationDate='2' } In: uuidKey, attribute={ ProtectStopDate='<*NOW+10min*>' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D7FE2477E364AE1A Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000000000002 (Thu Jan 01 01:00:02 CET Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 9696012991BC8A59 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B98E2B3 (Thu Mar 11 13:31:47 CET 42007801000001684200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004 2 4000000004200080100000028420 00A070000000F41637469766174696F6E204461746500420 00B090000000800000000000000 0242000F010 1150726F746563742053746F70204461746500000000000000042000B090000000800000000 4B98E2B3 Out: uuidKey, attribute={ ActivationDate='2' } Out: uuidKey, attribute={ ProtectStopDate='<*NOW+10min*>' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05B (Thu Mar 11 13:21:47 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)

	Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D7FE2477E364AE1A Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000000000002 (Thu Jan 01 01:00:02 CET Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 9696012991BC8A59 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B98E2B3 (Thu Mar 11 13:31:47 CET 42007B01000001984200 7A0100000484200690100000020420 06A0200000040000000100000000420 06B0200000040000000000000000420 6656264302D386562612D343036652D626532312D643930353965323962613164000000004200080100000028420 00A070000000F41637469 7 302D386562612D343036652D626532312D643930353965323962613164000000004200080100000030420 00A07000000011507 26F746563742 0
2	Client A: Add Attribute In: uuidKey, attribute={ UsageLimits={ UsageLimitsTotal='1000', UsageLimitsUnit='1'} } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Usage Limits Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Usage Limits Total (0x420097), Type: Long Integer (0x03), Data: 0x00000000000003E8 (1000) Tag: Usage Limits Unit (0x420098), Type: Enumeration (0x05), Data: 0x00000001 (Byte) 42007801000000D842007701000000384200690100000020420 06A0200000040000000100000000420 06B0200000040000000000000000420 70000000C5573616765204C696D69747300000000042000B0100000020420097030000000800000000000003E842009805000000040000000 10 Out: uuidKey, attribute={ UsageLimits={ UsageLimitsTotal= '1000', UsageLimitsCount='1000', UsageLimitsUnit='1'} } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

	Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05C (Thu Mar 11 13:21:48 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Usage Limits Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Usage Limits Total (0x420097), Type: Long Integer (0x03), Data: 0x00000000000003E8 (1000) Tag: Usage Limits Count (0x420096), Type: Long Integer (0x03), Data: 0x00000000000003E8 (1000) Tag: Usage Limits Unit (0x420098), Type: Enumeration (0x05), Data: 0x00000001 (Byte) 42007B01000001084200 7A01000000484200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000004 2 26532312D6439303539653239626131640000000042000801000000 5042000A070000000C5573616765204C696D6974730000000042000B010
3	Client B: Locate (symmetric key by name) In: objectType = ‘00000002’, attributes={ Name={ Name=‘Key1’, NameType= ‘00000001’} } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007801000000D0420077010000003842006901000000 2042006A020000000400000001000000004200 6B020000000400000000000000004 2 7000000044E616D650000000042000B0100000020420055070000000 44B65793100000000420054050000000400000001000000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

	Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05C (Thu Mar 11 13:21:48 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004226532312D643930353965323962613164000000
4	Client B: Get (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d 42007801000000904200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004242007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004226532312D643930353965323962613164000000 Out: objectType = ‘00000002’, uuidKey, symmetricKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05C (Thu Mar 11 13:21:48 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x420045), Type: Structure (0x01), Data:

	Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 674B32B1A3266DF1253B0F2C4440B0B0 Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128) 42007B01000001204200 7A01000000484200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000004 26656264302D386562612D343036652D626532312D643930353965323962613164000000000420 08F01000000584200400100000050420042050
5	Client B: Check Get usage allocation In (header): BatchOrderOption='true' In: uuidKey, UsageLimitsCount='500' In: uuidKey, UsageLimitsCount='500' Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000009 (Check) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 19D4F3DC9635307A Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d Tag: Usage Limits Count (0x420096), Type: Long Integer (0x03), Data: 0x00000000000001F4 (500) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 20C8DFFD55BDEEE8 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d Tag: Usage Limits Count (0x420096), Type: Long Integer (0x03), Data: 0x00000000000001F4 (500) 42007801000001204200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004 04000000042009603000000080000000000000001F442000F010000006842005C050000000400000011000000004200930800000000820C8DFFD5 Out: uuidKey Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05D (Thu Mar 11 13:21:49 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000009 (Check)

	Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 19D4F3DC9635307A Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 20C8DFFD55BDEEE8 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d 42007B01000001304200 7A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000004 2 6656264302D386562612D343036652D626532312D643930353965323962613164000000000420 00F01000000684200 5C050000000400000011 0
6	Client A: Get usage allocation In: uuidKey, UsageLimitsCount=’500’ Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d Tag: Usage Limits Count (0x420096), Type: Long Integer (0x03), Data: 0x00000000000001F4 (500) 4200780100000 0A0420077010000003842006901000000 2042006A020000000400000001000000042006B020000000400000000000000004 2 0000001F4 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05D (Thu Mar 11 13:21:49 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d 42007B01000000B042007A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000004 2

	26532312D6439303539653239626131640000000
7	Client C: Locate (symmetric key by name) In: objectType = '00000002', attributes={ Name={ Name='Key1', NameType='00000001'} } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007801000000D042007701000000384200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000004 27000000044E616D650000000042000B0100000020420055070000000 44B65793100000000420054050000000400000001000000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05D (Thu Mar 11 13:21:49 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004 26532312D6439303539653239626131640000000
8	Client C: Get (symmetric key) In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d
```

```
42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
```

Out: objectType = ‘00000002’, uuidKey, symmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05D (Thu Mar 11 13:21:49 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 674B32B1A3266DF1253B0F2C4440B0B0
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
```

```
42007B01000001204200 7A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000042
6656264302D386562612D343036652D626532312D643930353965323962613164000000000042008F010000005842004001000000504200420 50
```

9	Client C: Get usage allocation In: uuidKey, UsageLimitsCount=’500’

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
```

	Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d Tag: Usage Limits Count (0x420096), Type: Long Integer (0x03), Data: 0x00000000000001F4 (500) 42007801000000A042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000004200 0000001F4 Out: Operation Failed, Permission Denied Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05D (Thu Mar 11 13:21:49 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed) Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x0000000C (Permission Denied) Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Unable to allocate requested amount 42007B01000000B842007A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000004200 C6C6F6361746520726571756573746564206 16D6F756E740000000000
10	Client A: Revoke (symmetric key as cessation of operation) and Destroy (symmetric key) In (header): batchOrderOption='TRUE' In: uuidKey, revocationReasonCode='6' In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 727A212BC674B4EA Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data: Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000006 (Cessation of Operation Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

```
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 1D0EBF826109B0A5
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d
```

```
42007801000001284200770100000048420069010000002042006A020000000400000001000000004200
26532312D643930353965323962613164000000004200810100000010420082050000000400000006000
```

Out: uuidKey

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05F (Thu Mar 11 13:21:51 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 727A212BC674B4EA
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 1D0EBF826109B0A5
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29ba1d
```

```
42007B01000001304200 7A01000000484200690100000020420 6A020000000400000001000000004200
6656264302D386562612D343036652D626532312D643930353965323962613164000000004200 F010000006842005C05000000040000001 40
```

6 Key Interchange, Key Exchange

6.1 Use-case: Import of a Third-party Key

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

Time	Request/Response messages
0	Register (symmetric key)

	In: objectType = ‘00000002’, attributes={ CryptographicUsageMask=‘00000004’ }, foreignSymmetricKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
	  Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
	  Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt)
	  Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
	  Tag: Key Block (0x420040), Type: Structure (0x01), Data:
	  Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
	  Tag: Key Value (0x420045), Type: Structure (0x01), Data:
	  Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 0123456789ABCDEF0123456789ABCDEF
	  Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
	  Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
	
	42007801000001104200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004204D61736B42000B020000000400000004000000042008F010000058420040010000005042004205000000040000000100000000420045010
	
	Out: uuidKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED32 (Thu Nov 12 12:10:42 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7
	
	42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004223430642D393636663233316239316237000000000

1	Add attribute In: uuidKey, attribute={ x-provider=‘unknown’ } Tag: Request Message (0x420078), Type: Structure (0x01), Data:

	Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-provider Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: unknown 42007801000000C042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000004270000000A782D70726F76696465720000000000000042000B0700000007756E6B6E6F776E00 Out: uuidKey, attribute={ x-provider='unknown' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED32 (Thu Nov 12 12:10:42 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-provider Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: unknown 42007B01000000E042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004270000000A782D70726F76696465720000000000000042000B0700000007756E6B6E6F776E00
2	Modify attribute In: uuidKey, attribute={ x-provider='third party' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Request Payload (0x420079), Type: Structure (0x01), Data:

	Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-provider Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: third party 42007801000000C84200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042 70000000A782D70726F76696465720000000000042000B070000000B74686972642070617274790000000000 Out: uuidKey, attribute={ x-provider='third party' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED32 (Thu Nov 12 12:10:42 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-provider Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: third party 42007B01000000E842007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042 23430642D393636663233316239316237000000004200080100000030420 00A070000000A782D70726F76696465720000000000042000B070
3	Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

	Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED32 (Thu Nov 12 12:10:42 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004223430642D393636663233316239316237000000000

7 Vendor Extensions

These use-cases test the handling of unknown message extensions with vendor-specific content.

7.1 Use-case: Unrecognized Message Extension with Criticality Indicator false

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

Time	Client A
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMa Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128) Tag: Attribute (0x420008), Type: Structure (0x01), Data:

	Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt) Tag: Message Extension (0x420051), Type: Structure (0x01), Data: Tag: Criticality Indicator (0x420026), Type: Boolean (0x06), Data: FALSE Tag: Vendor Identification (0x42009D), Type: Text String (0x07), Data: Acme Tag: Vendor Extension (0x42009C), Type: Structure (0x01), Data: Tag: Unknown tag (0x014242), Type: Text String (0x07), Data: na 42007801000001604200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004280000000420008010000003042000A07000000174372797074 6F6772617068696320416C676F726 0441636D650000000042009C0100000001001424207000000026E61000000000000 Out: objectType='00000002', uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73BF1C (Thu Feb 11 09:26:04 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 052eff73-b35e-4702-9db9-37c12f0151d3 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004280000000420008010000003042000A07000000174372797074 6F6772617068696320416C676F726 5666637332D623335652D343730322D396462392D333763313266303135316433000000000
1	Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 052eff73-b35e-4702-9db9-37c12f0151d3 42007801000000904200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004280

	Out: uuidKey
	
	`Tag: Response Message (0x42007B), Type: Structure (0x01), Data:`
	`  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:`
	`  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)`
	`  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73BF1C (Thu Feb 11 09:26:04 CET 2010)`
	`  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:`
	`  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)`
	`  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)`
	`  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:`
	`  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 052eff73-b35e-4702-9db9-37c12f0151d3`
	
	`42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004296462392D33376331326630313531643300000000`

7.2 Use-case: Unrecognized Message Extension with Criticality Indicator true

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

Time	Client A

0	Create (symmetric key)
	In: objectType='00000002', attributes={ CryptographicAlgorithm='AES',
	CryptographicLength='128', CryptographicUsageMask='0000000C' }, MessageExtension={ VendorIdentification='Acme', Cr
	
	`Tag: Request Message (0x420078), Type: Structure (0x01), Data:`
	`  Tag: Request Header (0x420077), Type: Structure (0x01), Data:`
	`  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)`
	`  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:`
	`  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)`
	`  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:`
	`  Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)`
	`  Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:`
	`  Tag: Attribute (0x420008), Type: Structure (0x01), Data:`
	`  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length`
	`  Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)`

	Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt) Tag: Message Extension (0x420051), Type: Structure (0x01), Data: Tag: Criticality Indicator (0x420026), Type: Boolean (0x06), Data: TRUE Tag: Vendor Identification (0x42009D), Type: Text String (0x07), Data: Acme Tag: Vendor Extension (0x42009C), Type: Structure (0x01), Data: Tag: Unknown tag (0x014242), Type: Text String (0x07), Data: na 42007801000001604200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004280000000420 00B020000000400000008000000000420008010000003042000A07000000174372797074 6F6772617068696320416C676F726970 0441636D650000000042009C0100000010014242070000000026E61000000000000

Out: Operation Failed, Feature Not Supported

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73BF1D (Thu Feb 11 09:26:05 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)
    Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x00000008 (Feature Not Supported)
    Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Critical Message Extension not recognized

42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000004200
6B020000000400000000000000004280000000420
3736167652045787465 6E73696F6E206E6F74207265636F676E697A656400000000000000
```

8 Asymmetric keys

Creation of keys using “Create Key Pair” operation, locating pair using Link attribute.

8.1 Use-case: Create a Key Pair

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

Time	Client A
0	Create Key Pair

In: commonAttributes={ CryptographicAlgorithm='RSA', CryptographicLength='1024' }, privateKeyAttributes={ Name={ Nam

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000002 (Create Key Pair)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Common Template-Attribute (0x42001F), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (RSA)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000400 (1024)
      Tag: Private Key Template-Attribute (0x420065), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: PrivateKey1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000001 (Sign)
      Tag: Public Key Template-Attribute (0x42006E), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: PublicKey1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000002 (Verify)
```

```
42007801000001E84200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
40000000042000801000000342000A0700000014437279707 46F67726170686963204C656E6774680000000042000B020000000400000400 0
726170686963205573616765204D61736B42000B020000000400000001000000042006E01000000804200080100000040420 00A0700000004
00200000000
```

Out: uuidPrivateKey, uuidPublicKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
```

```
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13A (Thu Feb 11 09:35:06 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000002 (Create Key Pair)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-6dc2115cc042
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-879bab490259
```

```
42007B01000000E042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
93530342D3664633231313563633034320000000042009407000000246132343266361342D656266302D343339382D616336352D38373962
```

1 Locate (Public Key)

In: attributes={ objectType='PublicKey', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (Public Key)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000103 (Private Key Link)
          Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-879bab
```

```
42007801000000F042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000042
7000000044C696E6B0000000042000B010000004042004B050000000400000103000000000420 04C0700000024613234326663613 42D6562663
```

Out: uuidPublicKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13B (Thu Feb 11 09:35:07 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
```

	Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-6dc2115cc042 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004293530342D3664633231313563633034320000000 0
2	Locate (Private Key) In: attributes={ objectType='PrivateKey', Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Private Key) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000102 (Public Key Link) Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-6dc211 42007801000000F042007701000000384200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000004270000000044C696E6B0000000042000B010000004042004B0500000004000001020000000042004C0700000024383935663732633 22D6232306 Out: uuidPrivateKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13B (Thu Feb 11 09:35:07 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-879bab490259 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004216336352D3837396261623439303235390000000 0
3	Destroy In: uuidPrivateKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-879bab490259
```

```
42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
```

Out: uuidPrivateKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13B (Thu Feb 11 09:35:07 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-879bab490259
```

```
42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
16336352D383739626162343930323539000000000
```

4 Destroy

In: uuidPublicKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-6dc2115cc042
```

```
42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
```

Out: uuidPublicKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13B (Thu Feb 11 09:35:07 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-6dc2115cc042

42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
93530342D366463323131356363303432000000000
```

207

208 **8.2** Use-case: Register Both Halves of a Key Pair

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

211

Time	Client A

0	Register (Private Key)
	In: objectType='00000004', attributes={ CryptographicUsageMask='00000001' }, foreignPrivateKey
	
	`Tag: Request Message (0x420078), Type: Structure (0x01), Data:`
	`  Tag: Request Header (0x420077), Type: Structure (0x01), Data:`
	`  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)`
	`  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:`
	`  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)`
	`  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:`
	`  Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000004 (Private Key)`
	`  Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:`
	`  Tag: Attribute (0x420008), Type: Structure (0x01), Data:`
	`  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask`
	`  Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000001 (Sign)`
	`  Tag: Private Key (0x420064), Type: Structure (0x01), Data:`
	`  Tag: Key Block (0x420040), Type: Structure (0x01), Data:`
	`  Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000004`
	`  Tag: Key Value (0x420045), Type: Structure (0x01), Data:`
	`  Tag: Key Material (0x420043), Type: Octet String (0x08), Data:`
	`3082027602010030 0D06092A864886F70D0101010500048202603082025C02010002818100930451C9ECD94F5BB9DA17DD09381BD23BE43ECA`
	`C9F0203010001028180 0B6A7D736199EA48A420E4537CA0C7C046784DCBEAA63BAEBC0BC132787449CDE8D7CAD0C0C863C0FEFB06C3062BEFC`
	`AABC749FAA0DCD4C2583C71DDE8941A7B9AA030F52EF1451466C074D4D338FE677892ACD9E10FD35BD024100A98FBC3ED6B4C6F860F97165AC`

15FB5B3A9213463797AA9024100A1DDF023C0CD94C019BB26D09B9E3CA8FA971CB16AA58B9BAF79D6081A1DBBA452BA53653E2804BA98FF69E

```
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000004 (RSA)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000400 (1024)
```

```
42007801000003804200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004204
04D61736B42000B020000000400000001000000004200640100000 2C84200400100000 2C042004205000000040000000400000000420045010
2427E58ACCE7F6CE0F9BCC617BBD8C90D0094A2703BA0D09EB19D1005F2FB265526AAC75AF32F8BC782CDED2A57F811E03EAF67A944DE5E784
4599579F2100D65E038831FDAFB0DBE2BBDAC00A696E67E756350E1C99ACE11A36DABAC3ED3E730960059024100DDF672FBCC5BDA3D73AFFC4
49E204818A2F785F113F922B8B0240253F9470390D39049303777DDBC9750E9D64849CE0903EAE704DC9F589B7680DEB9D609FD5BCD4DECD6F
7FF974F688122365BF6690CDFC996E1890952EB3820DD1890EC1C8619E87A2BD38F9D03B37FAC742EFB748C7885942C390000000000004200 2
```

Out: uuidPrivateKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A1 (Thu Feb 11 09:49:37 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66d27b11943
```

```
42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004204
23661322D6436366432376231313934330000000 0
```

1

Register (Public Key)

In: objectType='00000004', attributes={ CryptographicUsageMask='00000002', Link={ LinkType='PrivateKeyLink', LinkedOb

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000003 (Public Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000002 (Verify)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000103 (Private Key Link)
            Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66c
```

	Tag: Public Key (0x42006D), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000005 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 30819F300D06092A864886F70D010101050003818D00308189028181009304 51C9ECD94F5BB9DA17DD09381BD23BE43ECA8C7539F301FC8A8C Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000004 (RSA) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000400 (1024) 42007801000002084200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004204D61736B42000B020000000400000002000000004200080100000058 42000A07000000044C696E6B0000000042000B010000004042004B050A230819F300D06092A864886F70D 010101050003818D00308189028181009304 51C9ECD94F5BB9DA17DD09381BD23BE43ECA8C7539F301FC8A0000000000004200280500000004000000040000000042002A020000000400000040000000000 Out: uuidPublicKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A2 (Thu Feb 11 09:49:38 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 79cbf228-16df-4fb1-a385-443546935e74 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004213338352D343433353436393335653734 00000000
2	Add attribute In: uuidPrivateKey, attribute={ Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66d27b11943 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:

Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000102 (Public Key Link)
Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: 79cbf228-16df-4fb1-a385-443546935e74

42007801000000F042007701000000384200690100000020420 06A020000000400000001000000004200 6B020000000400
43237623131393433000000004200080100000058420 00A07000000044C696E6B0000000042000B010000004042004B05

Out: uuidPrivateKey, attribute={ Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A2 (Thu Feb 11 09:49:38 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66d27b11943
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000102 (Public Key Link)
          Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: 79cbf228-16df-4fb1-a385-443546
```


```
42007B01000001104200 7A01000000484200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000004 2
23661322D6436366432376231313934330000000042000801000000584200 0A07000000044C696E6B0000000042000B010000004042004B050
```


3 Locate (Public Key)

In: attributes={ objectType='PublicKey', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (Public Key)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000103 (Private Key Link)
```

	Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66d27 42007801000000F042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000000427000000044C696E6B0000000042000B010000004042004B050000000400000103000000042004C0700000024666130363036386 32D3666623 Out: uuidPublicKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A2 (Thu Feb 11 09:49:38 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 79cbf228-16df-4fb1-a385-443546935e74 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004270000000 13338352D34343335343639333565373400000000
4	Locate (Private Key) In: attributes={ objectType='PrivateKey', Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Private Key) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000102 (Public Key Link) Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: 79cbf228-16df-4fb1-a385-443546 42007801000000F042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000004270000000 7000000044C696E6B0000000042000B010000004042004B050000000400000102000000042004C0700000024373963626632 32382D3136646 Out: uuidPrivateKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A3 (Thu Feb 11 09:49:39 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66d27b11943
```

```
42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004223661322D643636643237623131393343300000000
```

5 Destroy

In: uuidPrivateKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66d27b11943
```

```
42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004223661322D643636643237623131393343300000000
```

Out: uuidPrivateKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A3 (Thu Feb 11 09:49:39 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66d27b11943
```

```
42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004223661322D643636643237623131393343300000000
```

6	Destroy
	In: uuidPublicKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 79cbf228-16df-4fb1-a385-443546935e74
	
	42007801000000904200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004200
	
	Out: uuidPublicKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A3 (Thu Feb 11 09:49:39 CET 2010)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 79cbf228-16df-4fb1-a385-443546935e74
	
	42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004200
	13338352D34343335343639333565373400000000

212
213

214 9 Key Roll-over

215

216 These use-cases test manual key roll-over using the “Re-key” operation. In particular, they test the
217 formatting of the Re-key command, the handling and server-side processing of the various Time
218 attributes and the setting of some other attributes that are not automatically copied from the existing key
219 to the new key.

220 9.1 Use-case: Create a Key, Re-key

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

224

Time	Client A
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMa

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
```

```
42007801000001604200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
974686D0042000B0500000004000000030000000042000801000000304200 0A0700000144372797074 6F67726170686963204C656E6774680
204200550700000000872656B65794B65794200540500000004000000010000000 0
```

Out: objectType='00000002', uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BA (Thu Feb 11 10:07:06 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
```

	Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004263037333352D656636662D343038352D396530612D656236663133393463323138000000000
1	Locate In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007801000000A042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000004210000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BA (Thu Feb 11 10:07:06 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004296530612D656236663133393463323138000000000
2	Rekey In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data:

	Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004200 Out: uuidNewKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BB (Thu Feb 11 10:07:07 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: bf6cc1d4-f914-4099-b4d4-453050d8bcf4 42007B01000000B042007A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000004200 23464342D34353330353064386263663400000000
3	Locate In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007801000000A042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000004200 100000000

	Out: uuidNewKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BB (Thu Feb 11 10:07:07 CET 2010)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: bf6cc1d4-f914-4099-b4d4-453050d8bcf4
	
	42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000000423464342D34353330353064386263663400000000

4	Get Attribute
	In: uuidKey, attributeName={‘Name’}
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
	
	42007801000000A042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000004250000000
	
	Out: uuidKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BB (Thu Feb 11 10:07:07 CET 2010)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

	Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004296530612D656236663133393463323138000000
5	Get (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004 Out: objectType = ‘00000002’, uuidKey, symmetricKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BB (Thu Feb 11 10:07:07 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218 Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: BC25617991C49D06536008D076017462 Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128) 42007B01000001204200 7A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004263037333352D656636662D343038352D396530612D656236663133393463323138000000000042008F010000005842004001000000504200420500
6	Destroy In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218
```

```
42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BC (Thu Feb 11 10:07:08 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218
```

```
42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
96530612D6562366631333934633231380000000
```

7

Destroy

In: uuidNewKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: bf6cc1d4-f914-4099-b4d4-453050d8bcf4
```

```
42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
```

	Out: uuidNewKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BC (Thu Feb 11 10:07:08 CET 2010)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: bf6cc1d4-f914-4099-b4d4-453050d8bcf4
	
	42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004223464342D34353330353064386263663400000000

225

226

227 **9.2** Use-case: Existing Key Expired, Re-key with Same lifecycle

228 Create a new symmetric key. Then add the *Activation Date* and *Deactivation Date* attributes based on the
229 timestamp in the response to the Create request. The *Activation Date* is set to a time in the past and the
230 *Deactivation Date* to a time in the near future. Repeated Get Attribute calls are performed to verify that
231 the state is first “Active”, then subsequently “Deactivated”. Then issue a Re-key request, including an
232 *Activation Date* attribute with the value set to the previously specified *Deactivation Date* of the existing
233 key. Verify from the response that the *Activation Date* and *Deactivation Date* attributes were set correctly
234 (if they are not returned, issue a Get Attribute request). Do a Get Attribute operation to verify that the
235 state of the new key is “Active”. To clean up, both keys are deleted.

236

Time	Client A

0	Create (symmetric key)
	In: objectType=’00000002’, attributes={ CryptographicAlgorithm=’AES’,
	CryptographicLength=’128’, CryptographicUsageMask=‘0000000C’ }
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
	  Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:

	Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007801000001604200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004200974686D0042000B0500000004000000030000000042000801000000304200 0A07000000144372797074 6F6772617068696320 4C656E6774680020420055070000000872656B65794B65794200540500000004000000010000000 0 Out: objectType='00000002', uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73FFC7 (Thu Feb 11 14:01:59 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004200 5663365352D343862662D343239342D623735342D303537356134316439336236000000000
1	Add Activation Date, Deactivation Date attributes based on Timestamp in previous response (batch) In: uuidKey, attribute={ ActivationDate=' <*Timestamp in previous response – 365 days*>' } In: uuidKey, attribute={ DeactivationDate='<*Timestamp in previous response + 2 minutes*>' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

```
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BAC4A9CECC650259
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004992CC47 (Wed Feb 11 14:01:59 CET
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 582C952324F4552F
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B74003F (Thu Feb 11 14:03:59 CET
```

```
42007801000001784200770100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004223735342D3035373561343164393362360000000042000801000000284200A070000000F41637469766174696F6E204461746500420008010000003042000A07000000114465616374697766174696F6E204461746500000000000000042000B090000000800000004B74003F
```

Out: uuidKey, attribute={ ActivationDate=' <*Timestamp in previous response - 1 year*>' }

Out: uuidKey, attribute={ DeactivationDate=' <*Timestamp in previous response + 2 minutes*>' }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73FFC7 (Thu Feb 11 14:01:59 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BAC4A9CECC650259
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004992CC47 (Wed Feb 11 14:01:59 CET
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 582C952324F4552F
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B74003F (Thu Feb 11 14:03:59 CET
```

	42007B01000001984200 7A01000000484200690100000020420 06A02000000040000000100000000420 06B02000000040000000000000000420 5663365352D343862662D343239342D623735342D303537356134316439336236000000004200080100000028420 00A070000000F41637469 352D343862662D343239342D623735342D303537356134316439336236000000004200080100000030420 00A07000000114465616374697661
2	Get Attribute * *Repeated until state changes to Deactivated* In: uuidKey, attributeName={'State'} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 42007801000000A04200770100000038420069010000002042006A02000000040000000100000000420 06B02000000040000000000000000420 465000000 Out: uuidKey, attribute={ State='*Active*' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73FFC7 (Thu Feb 11 14:01:59 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active) 42007B01000000D842007A01000000484200690100000020420 06A02000000040000000100000000420 06B02000000040000000000000000420 23735342D303537356134316439336236000000004200080100000020420 00A070000000553746174650000004200 0B05000000040000000200
3	Get Attribute In: uuidKey, attributeName={'State'} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

```
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
```

```
42007801000000A042007701000000384200690100000020420 06A02000000040000000100000000420 06B020000000400000000000000004246
5000000
```

Out: uuidKey, attribute={ State='*Deactivated*' }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11 14:04:00 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (Deactivated)
```

```
42007B01000000D842007A0100000048420069010000002042006A020000000400000001000000004200 6B020000004000000000000000004246
23735342D3035373561343164393362360000000042000801000000204200 0A07000000055374617465000000420 00B05000000040000000300
```

4 Rekey

In: uuidKey, attribute={ offset='FE747E00' *(300 days backwards)*}

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6
      Tag: Offset (0x420058), Type: Interval (0x0A), Data: 0xFE747E00
```

```
42007801000000A042007701000000384200690100000020420 06A02000000040000000100000000420 06B020000000400000000000000004246
000000000
```

Out: uuidNewKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11 14:04:00 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92
```

```
42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000000042
23561332D6333373839653766326339320000000
```

5 Get Attribute

In: uuidNewKey, attributeName={‘ ActivationDate’, ‘DectivationDate’ }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date
```

```
42007801000000C84200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000000042
9766174696F6E20446174650042000A0700000011446561637469766174696F6E204461746500000000000000
```

Out: uuidNewKey, attribute={ ActivationDate=’ <*Value of ActivationTime in existing key + 65 days*>’, DectivationDate=’<*Valu*

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11 14:04:00 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
```

```
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000049E87DC6 (Fri Apr 17 15:01:58 CES
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004BC9B1BE (Sat Apr 17 15:03:58 CES

42007B01000001184200 7A01000000484200690100000020420 06A0200000040000000100000000420 06B020000000400000000000000004 2
23561332D6333373839653766326339320000000042000801000000284200 0A070000000F41637469766174696F6E20446174650042000B090
```

6 Get Attribute

In: uuidNewKey, attributeName={'State'}

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

4200780100000 0A0420077010000003842006901000000 2042006A0200000040000000100000000420 06B020000000400000000000000004 2
465000000
```

Out: uuidNewKey, attribute={ State='*Active*' }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11 14:04:00 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active)

42007B01000000D842007A01000000484200690100000020420 06A0200000040000000100000000420 06B020000000400000000000000004 2
```

	23561332D6333373839653766326339320000000042000801000000204200 0A0700000005537461746500000042000B0500000004000000020

7	Destroy
	In: uuidKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6
	
	42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
	
	Out: uuidKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11 14:04:00 CET 2010)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6
	
	42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
	23735342D3035373561343164393362360000000

8	Revoke (symmetric key as cessation of operation) and Destroy
	In (header): batchOrderOption='TRUE'
	In: uuidKey, revocationReasonCode='6'
	In: uuidNewKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

```
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7012417AA1B7394B
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92
      Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:
        Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000006 (Cessation of Operation
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3F8F4F1759704555
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92
```

```
42007801000001284200770100000048420069010000002042006A020000000400000001000000004200
23561332D633337383965376632633932000000004200810100000010420082050000000400000006000
```

Out: uuidNewKey

Out: uuidNewKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11 14:04:00 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7012417AA1B7394B
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3F8F4F1759704555
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92
```

```
42007B01000001304200 7A01000000484200690100000020420 06A020000000400000001000000004200
6303262312D636130322D346333632D623561332D633337383965376632633932000000004200 0F010000006842005C050000000400000014 0
```

9.3 Use-case: Existing Key Compromised, Re-key with same lifecycle

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

Time	Client A

0	Create (symmetric key)
	In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMa
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
	  Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
	  Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
	  Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
	  Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
	  Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B741047 (Thu Feb 11 15:12:23 C
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
	  Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
	  Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey
	  Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
	
	42007801000001904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
	974686D0042000B0500000004000000030000000042000801000000304200 0A0700000014437279707 46F67726170686963204C656E6774680
	0042000B090000000800000004B741047420008010000003842000A07000000044E616D650000000042000B0100000020420055070000000 8
	
	Out: objectType='00000002', uuidKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741048 (Thu Feb 11 15:12:24 CET 2010)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)

	Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004273432623423933665642D343233382D616664322D353331383963373966373831000000000
1	Get Attribute In: uuidKey, attributeName={'State'} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 42007801000000A042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000004246500000 Out: uuidKey, attribute={ State='*Active*' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741048 (Thu Feb 11 15:12:24 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active) 42007B01000000D842007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004216664322D353331383963373966373831000000004200080100000020420 0A0700000005537461746500000042000B050000000400000002
2	Revoke (symmetric key as compromised) In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceDate='*<NOW>*'

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781
      Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:
        Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000002 (Key Compromise)
      Tag: Compromise Occurrence Date (0x420021), Type: Date-Time (0x09), Data: 0x000000004B741048 (Thu Feb 11 15:
```

```
42007801000000B84200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000000420
50000000400000002000000004200210900000008000000004B741048
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11 15:12:25 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781
```

```
42007B01000000B042007A010000004842006901000000204200 6A020000000400000001000000042006B020000000400000000000000004200
16664322D353331383963373966373831000000000
```

3 Get Attribute

In: uuidKey, attributeName={‘State’}

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
```

	42007801000000A042007701000000384200690100000020420 06A02000000040000000100000000420 06B02000000040000000000000000420 0465000000 Out: uuidKey, attribute={ State='*Compromised*' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11 15:12:25 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Compromised) 42007B01000000D842007A0100000048420069010000002042006A020000000400000001000000004200 6B02000000040000000000000000420 0416664322D353331383963373966373831000000004200080100000020420 00A0700000005537461746500000042000B05000000040000000400
4	Rekey In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781 42007801000000904200770100000038420069010000002042006A020000000400000001000000004200 6B02000000040000000000000000420 0 Out: uuidNewKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11 15:12:25 CET 2010)

	Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-6ea36a801824 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004213633342D3665613336613830313832340000000
5	Get Attribute In: uuidNewKey, attributeName={'State'} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-6ea36a801824 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 4200780100000A042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000004213633342D3665613336613830313832340000000 Out: uuidNewKey, attribute={ State='*Active*' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11 15:12:25 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-6ea36a801824 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active) 42007B01000000D842007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004213633342D3665613336613830313832340000000004200080100000002042000A07000000055374617465000000042000B050000000400000002
6	Destroy

	In: uuidKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781
	
	42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004 2
	
	Out: uuidKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11 15:12:25 CET 2010)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781
	
	42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004 2
	16664322D353331383963373966373831000000000

7	Revoke (symmetric key as cessation of operation) and Destroy
	In (header): batchOrderOption='TRUE'
	In: uuidNewKey, revocationReasonCode='6'
	In: uuidNewKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
	  Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7131695CF636735E

```
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-6ea36a801824
      Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:
        Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000006 (Cessation of Operation
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 1845BCBBF09B5A66
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-6ea36a801824
```

```
42007801000001284200770100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004213633342D366561333661383031383234000000004200810100000010420082050000000400000006000000004200F0100000058420
```

Out: uuidNewKey

Out: uuidNewKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11 15:12:25 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7131695CF636735E
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-6ea36a801824
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 1845BCBBF09B5A66
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-6ea36a801824
```

```
42007B01000001304200 7A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000004213623737342D643030642D343539312D613633342D366561333661383031383234000000004200F0100000068420 05C050000000400000014
```

245

246

247 **9.4** Use-case: Create key, Re-key with new lifecycle

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

251

Time	Client A

0

Create (symmetric key)

In: objectType=’00000002’, attributes={ CryptographicAlgorithm=’AES’, CryptographicLength=’128’, CryptographicUsageMa

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
```

```
42007801000001604200770100000038420069010000002042006A020000000400000001000000004200
974686D0042000B0500000004000000030000000042000801000000304200
2042005507000000872656B65794B65794200540500000004000000010000
```

Out: objectType=’00000002’, uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742475 (Thu Feb 11 16:38:29 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef
```

	42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004243232539302D663738612D346433342D613266342D346436666338356135366566000000000
1	Locate In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007801000000A042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000004243232539302D663738612D346433342D613266342D346436666338356135366566000000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742476 (Thu Feb 11 16:38:30 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004243232539302D663738612D346433342D613266342D346436666338356135366566000000000
2	Rekey In: uuidKey, attributes={ ActivationDate='0000000043B7B630', ProcessStartDate='0000000043B7B630', ProtectStopDate=' Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

	Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000043B7B630 (Sun Jan 01 12:00:00 C Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Process Start Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000043B7B630 (Sun Jan 01 12:00:00 C Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000005E0C7BB0 (Wed Jan 01 12:00:00 C Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000005E0C7BB0 (Wed Jan 01 12:00:00 C 42007801000001704200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042 10000002842000A070000000F41637469766174696F6E20446174650042000B090000000800000043B7B630420008010000003042000A070 3042000A0700000011446561637469766174696F6E20446174650000000000000042000B090000000800000005E0C7BB0 Out: uuidNewKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742477 (Thu Feb 11 16:38:31 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042 96431322D666636666661613735666264000000000
3	Get Attribute In: uuidKey, attributeName={‘Name’} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

	Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name 42007801000000A042007701000000384200690100000020420 06A02000000040000000100000000420 06B02000000040000000000000000420 0500000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742477 (Thu Feb 11 16:38:31 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef 42007B01000000B042007A01000000484200690100000020420 06A02000000040000000100000000420 06B02000000040000000000000000420 13266342D34643666633835613536656600000000
4	Get Attribute In: uuidKey, attributeName={ ‘ActivationDate’, ‘ProcessStartDate’, ‘ProtectStopDate’, ‘DeactivationDate’ } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Process Start Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date 42007801000001084200770100000038420069010000002042006A02000000040000000100000000420 06B02000000040000000000000000420 9766174696F6E204461746500420 00A07000000125072 6F6365737320537461727420446174650000000000000420 00A07000000115072 6F746

Out: uuidKey, attribute={ ActivationDate='0000000043B7B630', ProcessStartDate='0000000043B7B630', ProtectStopDate=

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742477 (Thu Feb 11 16:38:31 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000043B7B630 (Sun Jan 01 12:00:00 CET
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Process Start Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000043B7B630 (Sun Jan 01 12:00:00 CET
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000005E0C7BB0 (Wed Jan 01 12:00:00 CET
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000005E0C7BB0 (Wed Jan 01 12:00:00 CET
```

```
42007B01000001884200 7A01000000484200690100000020420 06A02000000040000000100000000420 06B020000000400000000000000004 2
96431322D666636666666161373566626400000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B090
0042000B0900000008000000005E0C7BB0420008010000003042000A0700000011446561637469766174696F6E20446174650000000000000000
```

5 Locate

In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey
          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
```

```
4200780100000 0A042007701000000384200690100000020420 06A02000000040000000100000000420 06B020000000400000000000000004 2
```

	100000000
	
	Out: uuidNewKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742477 (Thu Feb 11 16:38:31 CET 2010)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd
	
	42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000000420
	96431322D666636666666161373566626400000000

6	Destroy
	In: uuidKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef
	
	42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000000420
	
	Out: uuidKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742478 (Thu Feb 11 16:38:32 CET 2010)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

	Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef 42007B01000000B042007A01000000484200690100000020420 06A02000000040000000100000000420 06B020000000400000000000000004213266342D346436666338356135366566000000000
7	Revoke (symmetric key as cessation of operation) and Destroy In (header): batchOrderOption='TRUE' In: uuidNewKey, revocationReasonCode='6' In: uuidNewKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3DC816BB39869D07 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data: Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000006 (Cessation of Operation Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 32B517312FD5B558 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd 42007801000001284200770100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004296431322D666636666666161373566626400000000420081010000001042008205000000040000000600000000420 0F010000005842005C050 Out: uuidNewKey Out: uuidNewKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742478 (Thu Feb 11 16:38:32 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3DC816BB39869D07 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

	Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 32B517312FD5B558 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd 42007B01000001304200 7A01000000484200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000004200 1366535632D313339372D346162342D396431322D666636666661613735666264000000004200 0F010000006842005C050000000400000014

252

253

254 **9.5** Use-case: Obtain Lease for Expired Key

255 Create a symmetric key with a specific name and obtain a lease. Revoke the key with state
256 “Compromised” and re-key the key. Try to obtain a lease on the old key which fails. Locate the new key
257 with the original name. Get the new key and obtain a lease.

258

Time	Client
0	Client A: Create (symmetric key) In: objectType=’00000002’, attributes={ CryptographicAlgorithm=’AES’, CryptographicLength=’128’, CryptographicUsageMask=‘0000000C’, Name={ NameValue=‘ rekeyKey’, NameType=’000000 Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name

	Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B74262C (Thu Feb 11 16:45:48 C 42007801000001904200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004 2 974686D0042000B0500000000400000003000000004200080100000030420 0A0700000014437279707 46F67726170686963204C656E6774680 2042005507000000087265 6B65794B65794200540500000004000000010000000042000801000000284200 0A070000000F4163746976617469
	Out: objectType='00000002', uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262D (Thu Feb 11 16:45:49 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004 2 6386533332D646333642D346337632D386636642D323632383935626333316365000000000
1	Client A: Get (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce 42007801000000904200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000004 2 Out: objectType = '00000002', uuidKey, symmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262D (Thu Feb 11 16:45:49 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data: F43C7798AACB22B1411A8773C199708B
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

42007B010000012042007A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000004 2
6386533332D646333642D346337632D386636642D323632383935626333316365000000000 42008F01000000584200400100000050420042050
```

2

Client A:

Obtain Lease

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce

420078010000009042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000004 2
```

Out: uuidKey, leaseTime, lastChangeDate

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262E (Thu Feb 11 16:45:50 CET 2010)
```

	Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce Tag: Lease Time (0x420049), Type: Interval (0x0A), Data: 0x00000010 Tag: Last Change Date (0x420048), Type: Date-Time (0x09), Data: 0x000000004B74262D (Thu Feb 11 16:45:49 CET 42007B01000000D042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042 86636642D32363238393562633331636500000004200490A000000040000001000000000420048090000000800000004B74262D
3	Client B: Revoke (symmetric key as compromised) In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceDate='<*NOW*>' Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data: Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000002 (Key Compromise) Tag: Compromise Occurrence Date (0x420021), Type: Date-Time (0x09), Data: 0x000000004B74262E (Thu Feb 11 16: 42007801000000B84200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042 50000000400000002000000004200210900000008000000004B74262E Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262E (Thu Feb 11 16:45:50 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042

	86636642D3236323839356263333163650000000

4	Client B:
	Rekey
	In: uuidKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce
	
	42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
	
	Out: uuidNewKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f
	
	42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
	93538312D37373835646335393366356600000000

5	Client A:
	Obtain Lease
	In: uuidKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)

	Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004 2 Out: Operation Failed, Permission Denied Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed) Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x0000000C (Permission Denied) Tag: Result Message (0x42007D), Type: Text String (0x07), Data: CO is in state Compromised, no lease given 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004 2 1746520436F6D70726F6D697365642C206E6F206C6561736520676976656E000000000000
6	Client A: Locate (symmetric key) In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007801000000A04200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004 2 100000000 Out: uuidNewKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

	Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004293538312D37373835646335393366356600000000
7	Client A: Get (symmetric key) In: uuidNewKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004 Out: objectType = ‘00000002’, uuidNewKey, newSymmetricKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001

	Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 173E9499F7C573712AFB9883B5DF2BCE Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128) 42007B01000001204200 7A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000042 2663831642D353734662D346634662D393538312D373738356463353933663566000000000420 08F0100000058420040010000005042004205 0
8	Client A: Obtain Lease In: uuidNewKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042 Out: uuidNewKey, leaseTime, lastChangeDate Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f Tag: Lease Time (0x420049), Type: Interval (0x0A), Data: 0x00000000 Tag: Last Change Date (0x420048), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 42007B01000000D042007A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000042 93538312D373738356463353933663566000000004200490A0000000400000000000000004200480900000008000000004B74262F
9	Client A: Destroy In: uuidKey

	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce
	
	42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004200
	
	Out: uuidKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce
	
	42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004200
	86636642D32363238393562633331636500000000

10	Client A:
	Revoke (symmetric key as cessation of operation) and Destroy
	In (header): batchOrderOption=’TRUE’
	In: uuidNewKey, revocationReasonCode=’6’
	In: uuidNewKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
	  Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3748B9E243205BA7
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:

```
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f
      Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:
        Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000006 (Cessation of Operation
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 04EAF416D0BEB50D
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f
```

```
42007801000001284200770100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
93538312D373738356463353933663566000000004200810100000010420082050000000400000006000000042000F010000005842005C050
```

Out: uuidNewKey

Out: uuidNewKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3748B9E243205BA7
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 04EAF416D0BEB50D
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f
```

```
42007B01000001304200 7A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000042
2663831642D353734662D346634662D393538312D373738356463353933663566000000004200F010000006842005C050000000400000014 0
```

10 Archival

These use-cases test archiving and locating keys using the off-line indicator. If the server performs the Archive and Recover operations asynchronously, the client Polls the server until the operations complete. The client indicates in the request that it supports asynchronous responses.

10.1 Use-case: Create a Key, Archive and Recover it

Create a symmetric key with a specified name, then use Locate to find the key and get the key. Archive the key (asynchronous operation, use Poll until it completes) and use Get and Locate on it, but both fail.

268 Add the Storage Status Mask to the Locate-command, indicating to the server to search in both online
269 and archived storage. The Locate finds the key. Recover the key from the archive (also asynchronous),
270 both Locate and Get succeed.

271

Time	Client A
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMa

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: archiveKey
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
```

```
420078010000016842007701000000384200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000004 2
974686D0042000B050000000400000003000000004200080100000030420 00A0700000014437279707 46F67726170686963204C656E6774680
2842005507000000 0A61726368697665 4B6579000000000000420054050000000400000001000000 00
```

Out: objectType='00000002', uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FA3 (Fri Feb 12 10:30:11 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
```

	Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000000425323136302D666230342D346637632D386137332D666566393035623231633066000000000
1	Locate In: attributes={ Name={ NameValue='archiveKey', NameType='00000001' } } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: archiveKey Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007801000000D842007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000000427000000044E616D650000000042000B0100000028420055070000000A617263686976654B65790000000000004200540500000004000000010 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FA6 (Fri Feb 12 10:30:14 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000000425 86137332D666566393035623231633066000000000

2	Get (symmetric key)
	In: uuidKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
	
	42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
	
	Out: objectType = ‘00000002’, uuidKey, symmetricKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FA7 (Fri Feb 12 10:30:15 CET 2010)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
	  Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
	  Tag: Key Block (0x420040), Type: Structure (0x01), Data:
	  Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
	  Tag: Key Value (0x420045), Type: Structure (0x01), Data:
	  Tag: Key Material (0x420043), Type: Octet String (0x08), Data: C3200B1291BA648DB9089DED3073DE74
	  Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
	  Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
	
	42007B01000001204200 7A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000042
	5323136302D666230342D346637632D386137332D666566393035623231633066000000000042008F010000005842004001000000542004205

3	Archive
	In: uuidKey, asynchronousIndicator=’true’
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

	Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000015 (Archive) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f 42007801000000A042007701000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000004260000000 Out: asynchronousCorrelationValue Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FA7 (Fri Feb 12 10:30:15 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000015 (Archive) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Operation Pending) Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: F17893DB51652969 42007B01000000884200 7A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004260000000
4	Poll* In: asynchronousCorrelationValue Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: F17893DB51652969 42007801000000704200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004260000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

	Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAA (Fri Feb 12 10:30:18 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000015 (Archive) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004286137332D6665663930356232316330660000000
5	Get (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000004 Out: Operation Failed, Object Archived Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAC (Fri Feb 12 10:30:20 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed) Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x0000000D (Object Archived) Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Object is archived 42007B01000000A842007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004226368697665640000000000000
6	Get Attribute (Archive Date) In: uuidKey, attributeName='ArchiveDate'

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Archive Date
```

```
42007801000000A84200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
8697665204461746500000000
```

Out: uuidKey, attribute={ ArchiveDate }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAC (Fri Feb 12 10:30:20 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Archive Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B751FAA (Fri Feb 12 10:30:18 CET
```

```
42007B01000000E042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
86137332D6665663930356232316330660000000042000801000000284200 0A070000000C41726368697665204461746500000000042000B090
```

7 Locate

In: attributes={ Name={ NameValue='archiveKey', NameType='00000001' } }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
```

```
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Name Value (0x420055), Type: Text String (0x07), Data: archiveKey
          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
```

```
42007801000000D84200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
7000000044E616D650000000042000B01000000284200550700000000A617263686976654B65790000000000000420054050000000400000001C
```

Out: <empty response payload>

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAC (Fri Feb 12 10:30:20 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: null
```

```
42007B01000000804200 7A01000000484200690100000020420 6A020000004000000010000000042006B020000000400000000000000042
```

8 Locate

In: storageStatusMask='00000003', attributes={ Name={ NameValue='archiveKey', NameType='00000001' } }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Storage Status Mask (0x42008E), Type: Integer (0x02), Data: 0x00000003 (3)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Name Value (0x420055), Type: Text String (0x07), Data: archiveKey
          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
```

```
42007801000000E84200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042
2000000004200080100000040420000A07000000044E616D650000000042000B01000000284200550700000000A617263686976654B657900000
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAC (Fri Feb 12 10:30:20 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
```

```
42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
86137332D6665663930356232316330660000000
```

9 Recover

In: uuidKey, asynchronousIndicator='true'

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000016 (Recover)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
```

```
42007801000000A042007701000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000042
600000000
```

Out: asynchronousCorrelationValue

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAC (Fri Feb 12 10:30:20 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
```

	Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000016 (Recover) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Operation Pending) Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: DDBB075607727F3F 42007B01000000842007A01000000484200690100000020420 06A0200000040000000100000000420 06B0200000040000000000000000420
10	Poll* In: asynchronousCorrelationValue Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: DDBB075607727F3F 42007801000000704200770100000038420069010000002042006A0200000040000000100000000420 06B0200000040000000000000000420 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FB3 (Fri Feb 12 10:30:27 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000016 (Recover) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f 42007B01000000B042007A01000000484200690100000020420 06A0200000040000000100000000420 06B0200000040000000000000000420 86137332D6665663930356232316330660000000
11	Get (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

```
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
```

```
42007801000000904200770100000038420069010000002042006A020000000400000001000000004200
6B020000000400000000000000004200
```

Out: objectType = '00000002', uuidKey, symmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FB3 (Fri Feb 12 10:30:27 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data: C3200B1291BA648DB9089DED3073DE74
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
```

```
42007B01000001204200
7A01000000484200690100000020420
06A020000000400000001000000004200
6B020000000400000000000000004200
5323136302D666230342D346637632D386137332D666566393035623231633066000000004200
8F010000005842004001000000504200
42050
```

12	Destroy In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
```

```
42007801000000904200770100000038420069010000002042006A020000000400000001000000004200
6B020000000400000000000000004200
```

	Out: uuidKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FB4 (Fri Feb 12 10:30:28 CET 2010)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
	
	42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004286137332D666566393035623231633066600000000

11 Access Control, Policies

These use-cases test attributes and objects related to access control and server policy.

11.1 Use-case: Credential, Operation Policy, Destroy Date

Pass a Credential object in the message header in all requests for identification purposes (how the Credential object is used is defined in OASIS Committee Specification 01, Key Management Interoperability Protocol Specification Version 1.0, June 2010, http://docs.oasis-open.org/kmip/spec/v1.0/cs01/kmip-spec-1.0-cs-01.doc **[KMIP-Prof]**). Create a symmetric key and set the Operation Policy Name attribute to “default”. Using another Credential, attempt to perform a Get operation batched with a Get Atttribute List on the created symmetric key – according to the Default Operation Policy, both these request SHALL fail, and with the Batch Error Continuation Option set to “Continue”, the client SHALL also receive both response payloads. Using the initially used Credential, destroy the object and get the Destroy Date attribute.

The message exchanges in this use case are based on a certain server policy (e.g. handling of Credentials) that in some aspects differs from the policy assumed in earlier use cases (e.g. in this use case, the Destroy Date is retained). As mentioned in Section 1 , the message exchanges shown in this document are not the only correct alternatives.

Time	Request/Response
0	Create (symmetric key) In (header): credential={ credentialType=’1’, credentialValue={ username=”Fred”, password=”password1” } } In: objectType=’00000002’, attributes={ CryptographicAlgorithm=’AES’, CryptographicLength=’128’, CryptographicUsageMa OperationPolicyName=’default’, CryptographicParameters={ BlockCipherMode=’1’, PaddingMethod=’3’, HashingAlgorithm=

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Authentication (0x42000C), Type: Structure (0x01), Data:
      Tag: Credential (0x420023), Type: Structure (0x01), Data:
        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password)
        Tag: Credential Value (0x420025), Type: Structure (0x01), Data:
          Tag: Username (0x420099), Type: Text String (0x07), Data: Fred
          Tag: Password (0x4200A1), Type: Text String (0x07), Data: password1
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: PolicyKey
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Operation Policy Name
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: default
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Parameters
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Block Cipher Mode (0x420011), Type: Enumeration (0x05), Data: 0x00000001 (CBC)
            Tag: Padding Method (0x42005F), Type: Enumeration (0x05), Data: 0x00000003 (PKCS5)
            Tag: Hashing Algorithm (0x420038), Type: Enumeration (0x05), Data: 0x00000004 (SHA-1)


42007801000002504200770100000088420069010000002042006A020000000400000001000000004200
5000000040000000100000000420079010000001A042005705000000040000000200000000420091010000
3042000A0700000018437279707 46F6772617068696320557361676520 4D61736B42000B020000000400000
B0700000007646566617 56C7400420008010000005842000A0700000018437279707 46F6772617068696320506172616D6574657273420008
```

Out: objectType=’00000002’, uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
```

	Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B9F8B4B (Tue Mar 16 14:44:43 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042 7383631352D386236642D346337302D626332332D3864313634383137353535356200000000
1	Client A Get Attributes, Get In (header): credential={ credentialType='1', credentialValue={ username="Fred", password="password1" } } In: attributeName='Operation Policy Name' In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Authentication (0x42000C), Type: Structure (0x01), Data: Tag: Credential (0x420023), Type: Structure (0x01), Data: Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password) Tag: Credential Value (0x420025), Type: Structure (0x01), Data: Tag: Username (0x420099), Type: Text String (0x07), Data: Fred Tag: Password (0x4200A1), Type: Text String (0x07), Data: password1 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 4CBB6751574C4DA8 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Operation Policy Name Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 0EA05EE703DA997B Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b 42007801000001704200770100000088420069010000002042006A020000000400000001000000042006B020000000400000000000000042 5000000040000000B00000000420093080000000084CBB6751574C4DA84200790100000050420094070000002436333437383631352D3862366 304200940700000024363334373836313 52D386236642D346337302D626332332D3864313634383137353535356200000000

Out: attributes={ OperationPolicyName='Default' }
Out: objectType = '00000002', uuidKey, symmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B9F8B4C (Tue Mar 16 14:44:44 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 4CBB6751574C4DA8
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Operation Policy Name
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: default
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 0EA05EE703DA997B
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data: C520FCA4E681F7BFFB3523D71427D594
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
```

```
42007B01000001D842007A0100000048420069010000002042006A020000000400000001000000004200
7383631352D386236642D346337302D626332332D386431363438313735353562000000004200080100000
040000000200000000420094070000002436333437383631352D386236642D346337302D626332332D3864
```

2 Client B
Get (symmetric key), Get Attribute List
In (header): credential={ credentialType='1', credentialValue={ username="Barney", password="secret2" } }, BatchOrderOpt
In: uuidKey
In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
```

```
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Authentication (0x42000C), Type: Structure (0x01), Data:
      Tag: Credential (0x420023), Type: Structure (0x01), Data:
        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password)
        Tag: Credential Value (0x420025), Type: Structure (0x01), Data:
          Tag: Username (0x420099), Type: Text String (0x07), Data: Barney
          Tag: Password (0x4200A1), Type: Text String (0x07), Data: secret2
    Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE
    Tag: Batch Error Continuation Option (0x42000E), Type: Enumeration (0x05), Data: 0x00000001
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: E3E72D5A352687D8
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: A9A1D60B0C62ECAF
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b
```

```
42007801000001684200770100000A042006901000000204200 6A020000000400000001000000042006B020000000400000000000000004 2
200000004000000020000000042000F0100000058420 05C050000000400000000A0000000042009308000000008E3E72D5A352687D842007901 0
2436333437383631352D386236642D346337302D626332332D386431363438313735353562000000000
```

Out: Operation Failed, Permission Denied

Out: Operation Failed, Permission Denied

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B9F8B4D (Tue Mar 16 14:44:45 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: E3E72D5A352687D8
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)
    Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x0000000C (Permission Denied)
    Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Access denied
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: A9A1D60B0C62ECAF
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)
    Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x0000000C (Permission Denied)
    Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Access denied
```

```
42007B01000001104200 7A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004 2
```

	70000000D41636365737320646 56E6965640000004200 0F01000000584200 5C05000000040000000C0000000042009308000000 08A9A1D60B0
3	Destroy In (header): credential={ credentialType='1', credentialValue={ username="Fred", password="password1" } } In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Authentication (0x42000C), Type: Structure (0x01), Data: Tag: Credential (0x420023), Type: Structure (0x01), Data: Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password) Tag: Credential Value (0x420025), Type: Structure (0x01), Data: Tag: Username (0x420099), Type: Text String (0x07), Data: Fred Tag: Password (0x4200A1), Type: Text String (0x07), Data: password1 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b 42007801000000E042007701000000884200690100000020420 06A0200000040000000100000000420 06B0200000040000000000000000420 0500000004000000140000000042007901000000304200940700000024363334373836313 52D386236642D346337302D626332332D386431363 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B9F8B4D (Tue Mar 16 14:44:45 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b 42007B01000000B042007A0100000048420069010000002042006A0200000040000000100000000420 06B0200000040000000000000000420 0426332332D386431363438313735353562000000 00
4	Get Attributes In (header): credential={ credentialType='1', credentialValue={ username="Fred", password="password1" } } In: uuidKey, attributeNames={ 'Destroy Date' } Tag: Request Message (0x420078), Type: Structure (0x01), Data:

```
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Authentication (0x42000C), Type: Structure (0x01), Data:
      Tag: Credential (0x420023), Type: Structure (0x01), Data:
        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password)
        Tag: Credential Value (0x420025), Type: Structure (0x01), Data:
          Tag: Username (0x420099), Type: Text String (0x07), Data: Fred
          Tag: Password (0x4200A1), Type: Text String (0x07), Data: password1
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Destroy Date
```

```
42007801000000F84200770100000088420069010000002042006A020000000400000001000000042006B020000000400000000000000042
5000000040000000B00000000420079010000004842009407000000243633343738363135 2D386236642D346337302D626332332D386431363
```

Out: uuidKey, attributes={ DestroyDate=’ 0x000000004B9F8B4D’ }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B9F8B4E (Tue Mar 16 14:44:46 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Destroy Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B9F8B4D (Tue Mar 16 14:44:45 CET
```

```
42007B01000000E042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
26332332D386431363438313735353562000000004200080100000028420 00A070000000C44657374726F7920446174650000000042000B090
```

12 Query, Maximum Response Size

This use case tests the Query operation and the Maximum Response Size header field.

12.1 Use-case: Query, Maximum Response Size

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

Time	Request/Response

0	Query (operations, objects)
	In (header): maximumResponseSize='256'
	In: queryFunctions={ '00000001', '00000002' }
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Maximum Response Size (0x420050), Type: Integer (0x02), Data: 0x00000100 (256)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000018 (Query)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000001 (Operations)
	  Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000002 (Objects)
	
	42007801000000904200770100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004
	
	Out: Operation Failed, Response Too Large
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B7918AA (Mon Feb 15 10:49:30 CET 2010)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)
	  Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x00000002 (Response Too Large)
	  Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Response size: 568, Maximum Response Size indi
	
	42007B01000000C842007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000004
	0526573706F6E73652053697A6520696E6469636174656420696E2072657175756573743A203235360000000000

1	Query (operations, objects) In (header): maximumResponseSize='2048' In: queryFunctions={ '00000001', '00000002' }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Maximum Response Size (0x420050), Type: Integer (0x02), Data: 0x00000800 (2048)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000018 (Query)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000001 (Operations)
      Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000002 (Objects)

42007801000000904200770100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042
```

Out: operations, objects

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B7918AA (Mon Feb 15 10:49:30 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000018 (Query)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000002 (Create Key Pair)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000009 (Check)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000012 (Activate)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000015 (Archive)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000016 (Recover)
```

```
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000018 (Query)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000019 (Cancel)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll)
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Certificate)
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000003 (Public Key)
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000004 (Private Key)
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000006 (Template)


42007B01000002304200 7A0100000484200690100000204200 6A020000004000000010000000042006B020000004000000000000000042
20000000042005C050000000400000003000000042005C050000000400000004000000042005C050000000400000008000000042005C050
0042005C050000000400000010000000042005C050000000400000011000000042005C050000000400000012000000042005C050000000 4
70500000004000000010000000420057050000000400000002000000042005705000000040000000300000004200570500000004000000
```

303

304 13 Implementation Conformance

305 This document is intended to be informational only and as such has no conformance clauses. The
306 conformance requirements for the KMIP Specification can be found in the "KMIP Specification" document
307 itself, at the URL noted on the cover page of this document.

308

309

A. Acknowledgments

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

Original Authors of the initial contribution:

David Babcock, HP
Joseph Birr-Pixton, Thales/nCipher
Mathias Björkqvist, IBM (editor)
John Clark, HP
Stan Feather, HP
Jon Geater, nCipher
Bob Griffin, EMC
Robert Haas, IBM
Jack Harwood, EMC
Vlad Libershteyn, HP
Mark Lin, EMC/RSA
Brian Metzger, HP
Madhav Mutalik, EMC/RSA
Anthony Nadalin, IBM
René Pawlitzek, IBM (editor)
Bruce Rich, IBM
Parameswaran Seshan, EMC/RSA
John Tattan, EMC

Participants:

Mike Allen, PGP Corporation
Gordon Arnold, IBM
Todd Arnold, IBM
Matthew Ball, Oracle Corporation
Elaine Barker, NIST
Peter Bartok, Venafi, Inc.
Mathias Björkqvist, IBM
Kevin Bocek, Thales e-Security
Kelley Burgin, National Security Agency
Jon Callas, PGP Corporation
Tom Clifford, Symantec Corp.
Graydon Dodson, Lexmark International Inc.
Chris Dunn, SafeNet, Inc.
Paul Earsy, SafeNet, Inc.
Stan Feather, Hewlett-Packard
Indra Fitzgerald, Hewlett-Packard
Alan Frindell, SafeNet, Inc.
Judith Furlong, EMC Corporation
Jonathan Geater, Thales e-Security
Robert Griffin, EMC Corporation
Robert Haas, IBM
Thomas Hardjono, M.I.T.
Kurt Heberlein, 3PAR, Inc.
Marc Hocking, BeCrypt Ltd.
Larry Hofer, Emulex Corporation
Brandon Hoff, Emulex Corporation
Walt Hubis, LSI Corporation

Tim Hudson, Cryptsoft
Wyllys Ingersoll, Oracle Corporation
Jay Jacobs, Target Corporation
Glen Jaquette, IBM
Scott Kipp, Brocade Communications Systems, Inc.
David Lawson, Emulex Corporation
Hal Lockhart, Oracle Corporation
Robert Lockhart, Thales e-Security
Shyam Mankala, EMC Corporation
Upendra Mardikar, PayPal Inc.
Marc Massar, Individual
Don McAlister, Associate
Hyrum Mills, Mitre Corporation
Bob Nixon, Emulex Corporation
Landon Curt Noll, Cisco Systems, Inc.
René Pawlitzek, IBM
John Peck, IBM
Rob Philpott, EMC Corporation
Scott Rea, Individual
Bruce Rich, IBM
Scott Rotondo, Oracle Corporation
Saikat Saha, Vormetric, Inc.
Anil Saldhana, Red Hat
Subhash Sankuratripati, NetApp
Mark Schiller, Hewlett-Packard
Jitendra Singh, Brocade Communications Systems, Inc.
Servesh Singh, EMC Corporation
Terence Spies, Voltage Security
Sandy Stewart, Oracle Corporation
Marcus Streets, Thales e-Security
Brett Thompson, SafeNet, Inc.
Benjamin Tomhave, Individual
Sean Turner, IECA, Inc.
Paul Turner, Venafi, Inc.
Marko Vukolić, IBM
Rod Wideman, Quantum Corporation
Steven Wierenga, Hewlett-Packard
Peter Yee, EMC Corporation
Krishna Yellepeddy, IBM
Peter Zelechoski, Election Systems & Software
Grace Zhang, Skyworth TTG Holdings Limited

B. Revision History

Revision	Date	Editor	Changes Made
ed-0.98	2009-04-28	Mathias Björkqvist	Initial conversion of input document to OASIS format.
ed-0.98	2009-08-06	Mathias Björkqvist	Changes to layout and message content to reflect the recent changes to the KMIP specification, added descriptions to the use-cases for which they were missing.
ed-0.98	2009-09-28	Mathias Björkqvist	Updated messages and TTLV encodings to conform with KMIP specification ed-0.98 rev 17.
draft-01	2009-10-08	Mathias Björkqvist	Removed normative words “must”, “shall”, “required”, “will” and “can”; updated messages and TTLV encodings to conform to KMIP specification ed-0.98 rev 19; added normative references; added minor edits
draft-02	2009-10-15	Mathias Björkqvist	Replaced the TBDs, changed status to Committee Draft, changed use-cases to use protocol major version 1 and minor version 0
draft-03	2009-10-15	Mathias Björkqvist	Corrected names of TC chairs
draft-04	2009-11-05	Mathias Björkqvist	Added list of participants, added reference to Profiles document, line spacing change to list of original contributors, added related documents
cd-05	2009-11-06	Mathias Björkqvist	Changes to various naming aspects on front page and document footer. This is the tentative version for public review.
cd-06	2009-11-12	Mathias Björkqvist	Updated tags.
cd-07	2010-02-17	Mathias Björkqvist	Addressed public review comments, added line numbering.
cd-08	2010-03-17	Mathias Björkqvist	Registration of Templates changed to use the Template object, Usage Allocation changes (Add Attribute, Check, Get Usage Allocation), batched Revoke requests with Destroy requests when destroying objects in the Active state, adopted new format for Username and Password Credential object.
cd-09	2010-03-18	Mathias Björkqvist	Updated participants’ list. Editorial fixes.
cd-10	2010-05-25	Mathias Björkqvist	Addressed comments from second public review.
cd-11	2010-05-28	Mathias Björkqvist	Updated participants’ list. Updated cross-references to KMIP specs. Version used for Committee Specification.