



Key Management Interoperability Protocol Use Cases Version 1.0

Committee Draft 05 / Public Review 01

06 November 2009

Specification URIs:

This Version:

<http://docs.oasis-open.org/kmip/usecases/v1.0/cd05/kmip-usecases-1.0-cd-05.html>
<http://docs.oasis-open.org/kmip/usecases/v1.0/cd05/kmip-usecases-1.0-cd-05.doc> (Authoritative)
<http://docs.oasis-open.org/kmip/usecases/v1.0/cd05/kmip-usecases-1.0-cd-05.pdf>

Previous Version:

<http://docs.oasis-open.org/kmip/usecases/v1.0/cd04/kmip-usecases-1.0-draft-04.html>
<http://docs.oasis-open.org/kmip/usecases/v1.0/cd04/kmip-usecases-1.0-draft-04.doc>
(Authoritative)
<http://docs.oasis-open.org/kmip/usecases/v1.0/cd04/kmip-usecases-1.0-draft-04.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, <http://docs.oasis-open.org/kmip/spec/v1.0/>
- Key Management Interoperability Protocol Profiles Version 1.0, <http://docs.oasis-open.org/kmip/profiles/v1.0/>
- Key Management Interoperability Protocol Usage Guide Version 1.0, <http://docs.oasis-open.org/kmip/ug/v1.0/>

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

Copyright © OASIS® 2009. All Rights Reserved.

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

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

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

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

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

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

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

The names "OASIS", [insert specific trademarked names and abbreviations here] 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	5
1.1 Normative References	5
2 Message exchange	5
3 Centralized Management	5
3.1 Basic functionality	5
3.1.1 Use-case: Create / Destroy	5
3.1.2 Use-case: Register / Create / Get attributes / Destroy	8
3.1.3 Use-case: Create / Locate / Get / Destroy	13
3.1.4 Use-case: Dual client use-case, ID Placeholder linked Locate & Get batch	18
3.2 Use-case: Asynchronous Locate	33
4 Key life cycle support	43
4.1 Use-case: Revoke scenario	43
5 Auditing and reporting	60
5.1 Use-case: Get usage allocation scenario	60
6 Key Interchange, Key Exchange	72
6.1 Use-case: Import of a Third-party Key	72
7 Vendor Extensions	76
7.1 Use-case: Unrecognized Message Extension with Criticality Indicator false	76
7.2 Use-case: Unrecognized Message Extension with Criticality Indicator true	77
8 Asymmetric keys	77
8.1 Use-case: Create a Key Pair	77
8.2 Use-case: Register Both Halves of a Key Pair	78
9 Key Roll-over	79
9.1 Use-case: Create a Key, Re-key	79
9.2 Use-case: Existing Key Expired, Re-key with Same lifecycle	80
9.3 Use-case: Existing Key Compromised, Re-key with same lifecycle	81
9.4 Use-case: Create key, Re-key with new lifecycle	82
9.5 Use-case: Obtain Lease for Expired Key	83
10 Archival	84
10.1 Use-case: Create a Key, Archive and Recover it	84
A. Acknowledgments	86
B. Revision History	88

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 QA 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).

1.1 Normative References

- [KMIP-Spec]** OASIS Draft, *Key Management Interoperability Specification v1.0*, Committee Draft, November 2009.
- [KMIP-Prof]** OASIS Draft, *Key Management Interoperability Protocol Profiles v1.0*, Committee Draft, November 2009.

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 http transport. This is to facilitate debugging and to focus on KMIP-specific issues instead of potential secure transport setup problems.

3 Centralized Management

3.1 Basic functionality

These use-cases test the basic features of KMIP including key creation and template 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='0000002' (Symmetric Key), attributes={ CryptographicAlgorithm='0000003' (AES), CryptographicLength='128', CryptographicUsageMask='000000C' }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000001 (Create)
Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
Tag: Template-Attribute (0x42008E), 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)

420075010000012042007401000000384200670100000020420068020000004000000010000000420069020000004
000000000000000042000D0200000004000000010000000042000F01000000D842005A05000000040000000100000000
42007601000000C0420055050000000400000002000000042008E01000000A8420008010000003042000A0700000017
43727970746F6772617068696320416C676F726974686D0042000B050000000400000003000000004200080100000030
42000A070000001443727970746F67726170686963204C656E677468000000042000B02000000040000008000000000
420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004
0000000C00000000

Out: objectType='0000002', uuidKey

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: 0x000000004AC0731C (Mon Sep 28
10:26:04 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: 0x00000001 (Create)
Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

	<p>Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 46eca90a-4b20-423c-b968-750f299f0ca7</p> <p>42007801000000C0420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042008F0900000008000000004AC0731C42000D0200000004000000010000000042000F010000006842005A0500000004000000010000000042007C05000000040000000000000000420079010000004042005505000000040000000200000000420091070000002434366563613930612D346232302D343233632D623936382D37353066323939663063613700000000</p>
1	<p>Destroy (symmetric key) In: uuidKey</p> <p>Tag: Request Message (0x420075), Type: Structure (0x01), Data: Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420076), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 46eca90a-4b20-423c-b968-750f299f0ca7</p> <p>4200750100000090420074010000003842006701000000204200680200000004000000010000000042006902000000040000000000000042000D0200000004000000010000000042000F010000004842005A0500000004000000014000000004200760100000030420091070000002434366563613930612D346232302D343233632D623936382D37353066323939663063613700000000</p> <p>Out: uuidKey</p> <p>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: 0x000000004AC0731D (Mon Sep 28 10:26:05 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: 0x00000014 (Destroy) Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 46eca90a-4b20-423c-b968-750f299f0ca7</p> <p>42007801000000B0420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042008F0900000008000000004AC0731D42000D0200000004000000010000000042000F010000005842005A0500000004000000014000000042007C050000000400000000000000004200790100000030420091070000002434366563613930612D346232302D343233632D623936382D37353066323939663063613700000000</p>

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

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

Time	Request/Response messages
0	<p>Register (template)</p> <p>In: objectType='00000007', attributes={ ObjectGroup='Group1', ApplicationSpecificInformation='ssl, www.example.com', ContactInformation='Joe', x-Purpose='demonstration', Name={ NameValue='Template1', NameType='00000001' } }</p> <p>Tag: Request Message (0x420075), Type: Structure (0x01), Data:</p> <p> Tag: Request Header (0x420074), Type: Structure (0x01), Data:</p> <p> Tag: Protocol Version (0x420067), Type: Structure (0x01), Data:</p> <p> Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p> Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p> Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p> Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p> Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000003 (Register)</p> <p> Tag: Request Payload (0x420076), Type: Structure (0x01), Data:</p> <p> Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000006 (Template)</p> <p> Tag: Template-Attribute (0x42008E), Type: Structure (0x01), Data:</p> <p> Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p> Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group</p> <p> Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1</p> <p> Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p> Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Application Specific Information</p> <p> Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:</p> <p> Tag: Application Namespace (0x420003), Type: Text String (0x07), Data: ssl</p> <p> Tag: Application Data (0x420002), Type: Text String (0x07), Data: www.example.com</p> <p> Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p> Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information</p> <p> Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe</p> <p> Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p> Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-Purpose</p> <p> Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: demonstration</p> <p> Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p> Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name</p> <p> Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:</p> <p> Tag: Name Value (0x420053), Type: Text String (0x07), Data: Template1</p> <p> Tag: Name Type (0x420052), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)</p> <p>42007501000001C04200740100000038420067010000002042006802000000040000000100000004200690200000004000000000000042000D020000000400000001000000042000F010000017842005A0500000004000000030000000042007601000001604200550500000004000000060000000042008E0100000148420008010000002842000A070000000C4F626A6563742047726F7570000000042000B070000000647726F757031000420008010000005842000A07000000204170706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000B0100000028420003070000000373736C000000000420002070000000F7777772E6578616D706C652E636F6D00420008010000003042000A0700000013436F6E</p>

7461637420496E666F726D6174696F6E00000000042000B07000000034A6F6500000000420008010000003042000A0700000009782D507572706F7365000000000000042000B070000000D64656D6F6E7374726174696F6E000000420008010000004042000A07000000044E616D65000000042000B0100000028420053070000000954656D706C617465310000000000000042005205000000040000000100000000

Out: uuidTemplate

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: 0x000000004AC0731E (Mon Sep 28 10:26:06 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: 0x00000003 (Register)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fc3f473-4de4-4248-990e-21e00f7fc006

42007801000000B0420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042008F0900000008000000004AC0731E42000D0200000004000000010000000042000F010000005842005A0500000004000000030000000042007C050000000400000000000000000000420079010000003042009107000000243466333663437332D346465342D343234382D393930652D32316530306637666330303600000000

1

Create (symmetric key using template)
In: objectType='00000002', template={ NameValue='Template1', NameType='00000001' }, attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C' }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000001 (Create)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Template-Attribute (0x42008E), Type: Structure (0x01), Data:
 Tag: Name (0x420051), Type: Structure (0x01), Data:
 Tag: Name Value (0x420053), Type: Text String (0x07), Data: Template1
 Tag: Name Type (0x420052), 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:
Mask
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)

420075010000015042007401000000384200670100000020420068020000004000000010000000042006902000000040000000000000042000D0200000004000000010000000042000F010000010842005A0500000004000000010000000042007601000000F04200550500000004000000020000000042008E01000000D84200510100000028420053070000000954656D706C617465310000000000000042005205000000040000000100000000420008010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000A070000001443727970746F67726170686963204C656E6774680000000042000B020000000400000008000000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000040000000C00000000

Out: objectType='00000002', uuidKey

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: 0x000000004AC0731F (Mon Sep 28 10:26:07 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: 0x00000001 (Create)
Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 300881c8-596a-48ad-814f-7cell19896608

42007801000000C042007701000000484200670100000020420068020000004000000010000000042006902000000040000000000000042008F0900000008000000004AC0731F42000D0200000004000000010000000042000F010000006842005A0500000004000000010000000042007C05000000040000000000000000420079010000004042005505000000040000000200000000420091070000002433303038383163382D353936612D343861642D383134662D37636531313938393636303800000000

2 Get attributes
In: uuidKey, attributeNames={'ObjectGroup', 'ApplicationSpecificInformation', 'ContactInformation', 'x-Purpose'}
Tag: Request Message (0x420075), Type: Structure (0x01), Data:
Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 300881c8-596a-48ad-814f-7cell19896608

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

4200750100000108420074010000003842006701000000204200680200000040000000100000004200690200000040
0000000000000042000D020000000400000001000000042000F01000000C042005A05000000040000000B0000000042
007601000000A8420091070000002433303038383163382D353936612D343861642D383134662D3763653131393839363
63038000000042000A070000000C4F626A6563742047726F7570000000042000A07000000204170706C69636174696F
6E20537065636966696320496E666F726D6174696F6E42000A0700000013436F6E7461637420496E666F726D6174696F6
E00000000042000A0700000009782D507572706F736500000000000000

Out: uuidKey, attributes={ ObjectGroup='Group1', ApplicationSpecificInformation='ssl,
www.example.com', ContactInformation='Joe Miller', x-Purpose='demonstration' }

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: 0x000000004AC0731F (Mon Sep 28
10:26:07 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: 0x0000000B (Get Attributes)
Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 300881c8-596a-48ad-814f-
7cell98966608
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

42007801000001B0420077010000004842006701000000204200680200000040000000100000004200690200000040
0000000000000042008F0900000008000000004AC0731F42000D0200000004000000010000000042000F010000015842
005A05000000040000000B0000000042007C05000000040000000000000042007901000001304200910700000024333
03038383163382D353936612D343861642D383134662D3763653131393839363630380000000042000801000000284200
0A070000000C4F626A6563742047726F7570000000042000B070000000647726F7570310000420008010000005842000
A07000000204170706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000B0100000028420003
070000000373736C000000000420002070000000F7777772E6578616D706C652E636F6D00420008010000003042000A0
700000013436F6E7461637420496E666F726D6174696F6E000000000042000B07000000034A6F65000000000042000801

	<p>0000003042000A0700000009782D507572706F7365000000000000042000B070000000D64656D6F6E7374726174696F6E000000</p>
<p>3</p>	<p>Destroy (symmetric key) In: uuidKey</p> <p>Tag: Request Message (0x420075), Type: Structure (0x01), Data: Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420076), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 300881c8-596a-48ad-814f-7cell19896608</p> <p>420075010000009042007401000000384200670100000020420068020000000400000001000000004200690200000004000000000000042000D020000000400000001000000042000F010000004842005A050000000400000014000000004200760100000030420091070000002433303038383163382D353936612D343861642D383134662D37636531313938393636303800000000</p> <p>Out: uuidKey</p> <p>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: 0x000000004AC07320 (Mon Sep 28 10:26:08 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: 0x00000014 (Destroy) Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 300881c8-596a-48ad-814f-7cell19896608</p> <p>42007801000000B042007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000042008F0900000008000000004AC073204200D0200000004000000010000000042000F010000005842005A0500000004000000140000000042007C05000000040000000000000004200790100000030420091070000002433303038383163382D353936612D343861642D383134662D37636531313938393636303800000000</p>
<p>4</p>	<p>Destroy (template) In: uuidTemplate</p> <p>Tag: Request Message (0x420075), Type: Structure (0x01), Data: Tag: Request Header (0x420074), Type: Structure (0x01), Data: Tag: Protocol Version (0x420067), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000001 (1)</p>

```

Tag: Protocol Version Minor (0x420069), 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 (0x42005A), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
  Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
    Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fc3f473-4de4-4248-990e-21e00f7fc006

4200750100000090420074010000003842006701000000204200680200000004000000010000000042006902000000040
0000000000000042000D0200000004000000010000000042000F010000004842005A0500000004000000140000000042
00760100000030420091070000002434666333663437332D346465342D343234382D393930652D32316530306663766633
03036000000000

```

Out: uuidTemplate

```

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: 0x000000004AC07320 (Mon Sep 28
10:26:08 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: 0x00000014 (Destroy)
      Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
      Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
        Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fc3f473-4de4-4248-990e-21e00f7fc006

42007801000000B0420077010000004842006701000000204200680200000004000000010000000042006902000000040
0000000000000042008F0900000008000000004AC0732042000D0200000004000000010000000042000F010000005842
005A0500000004000000140000000042007C0500000004000000000000000042007901000000304200910700000024346
66333663437332D346465342D343234382D393930652D323165303066637666330303600000000

```

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='DES', CryptographicLength='56', CryptographicUsageMask='0000000C', ContactInformation='Joe' }

```

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
  Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
      Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x42008E), 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 (0x420053), Type: Text String (0x07), Data: Key1
            Tag: Name Type (0x420052), 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: 0x00000001 (DES)
          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: 0x00000038 (56)
          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

```

```

4200750100000198420074010000003842006701000000204200680200000004000000010000000042006902000000040
000000000000042000D0200000004000000010000000042000F010000015042005A0500000004000000010000000042
00760100000138420055050000000400000002000000042008E0100000120420008010000003842000A07000000044E6
16D650000000042000B010000002042005307000000044B65793100000000420052050000000400000001000000004200
08010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B050000000400000
00100000000420008010000003042000A070000001443727970746F67726170686963204C656E677468000000042000B
02000000040000003800000000420008010000003042000A070000001843727970746F677261706869632055736167652
04D61736B42000B02000000040000000C00000000420008010000003042000A0700000013436F6E7461637420496E666F
726D6174696F6E00000000042000B07000000034A6F650000000000

```

Out: objectType = '00000002', uuidKey

```

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: 0x000000004AC07321 (Mon Sep 28
10:26:09 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

```

Tag: Batch Item (0x4200F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000001 (Create)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 75da9bc9-7867-49c5-886d-757f3d523d3f

42007801000000C04200770100000048420067010000002042006802000000400000001000000004200690200000040
 000000000000000042008F0900000008000000004AC0732142000D02000000400000001000000004200F010000006842
 005A0500000004000000010000000042007C050000000400000000000000042007901000000404200550500000004000
 0000200000000420091070000002437356461396263392D373836372D343963352D383836642D37353766336435323364
 336600000000

1

Locate (symmetric key)
In: attributes={ objectType = '00000002', Name={ Name='Key1', NameType='00000001' } }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: 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: Request Payload (0x420076), 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 (0x420053), Type: Text String (0x07), Data: Key1
 Tag: Name Type (0x420052), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007501000000D04200740100000038420067010000002042006802000000400000001000000004200690200000040
 000000000000000042000D02000000400000001000000004200F010000008842005A0500000004000000080000000042
 0076010000007042008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000
 000020000000042008010000003842000A07000000044E616D650000000042000B010000002042005307000000044B65
 79310000000042005205000000040000000100000000

Out: uuidKey

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: 0x000000004AC07321 (Mon Sep 28 10:26:09 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:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 75da9bc9-7867-49c5-886d-757f3d523d3f

42007801000000B04200770100000048420067010000002042006802000000400000001000000004200690200000004000000000000042008F0900000008000000004AC0732142000D02000000400000001000000004200F010000005842005A0500000004000000080000000042007C050000000400000000000000042007901000000304200910700000002437356461396263392D373836372D343963352D383836642D37353766336435323364336600000000

2

Get (symmetric key)

In: uuidKey

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 75da9bc9-7867-49c5-886d-757f3d523d3f

42007501000000904200740100000038420067010000002042006802000000400000001000000004200690200000004000000000000042008F0100000004842005A05000000040000000A0000000042007C050000000304200910700000002437356461396263392D373836372D343963352D383836642D37353766336435323364336600000000

Out: objectType = '00000002', uuidKey, symmetricKey

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: 0x000000004AC07322 (Mon Sep 28 10:26:10 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: 0x0000000A (Get)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 75da9bc9-7867-49c5-886d-757f3d523d3f
 Tag: Symmetric Key (0x42008C), Type: Structure (0x01), Data:
 Tag: Key Block (0x42003E), Type: Structure (0x01), Data:

Tag: Key Format Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001
 Tag: Key Value (0x420043), Type: Structure (0x01), Data:
 Tag: Key Material (0x420041), Type: Octet String (0x08), Data: EAD09734B085DFFE
 Tag: Cryptographic Algorithm (0x420026), Type: Enumeration (0x05), Data: 0x00000001 (DES)
 Tag: Cryptographic Length (0x420028), Type: Integer (0x02), Data: 0x00000038 (56)

4200780100000118420077010000004842006701000000204200680200000004000000010000000042006902000000040
 0000000000000042008F0900000008000000004AC0732242000D020000000400000001000000004200F01000000C042
 005A05000000040000000A0000000042007C050000000400000000000000042007901000000984200550500000004000
 0000200000000420091070000002437356461396263392D373836372D343963352D383836642D37353766336435323364
 3366000000042008C010000005042003E010000004842004005000000040000000100000000420043010000001042004
 10800000008EAD09734B085DFFE420026050000000400000001000000004200280200000040000003800000000

3 **Destroy (symmetric key)**
In: uuidKey

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 75da9bc9-7867-49c5-886d-757f3d523d3f

4200750100000090420074010000003842006701000000204200680200000004000000010000000042006902000000040
 0000000000000042000D0200000004000000010000000042000F010000004842005A0500000004000000140000000042
 00760100000030420091070000002437356461396263392D373836372D343963352D383836642D3735376633643532336
 43366000000000

Out: uuidKey

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: 0x000000004AC07322 (Mon Sep 28 10:26:10 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: 0x00000014 (Destroy)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 75da9bc9-7867-49c5-886d-757f3d523d3f

42007801000000B0420077010000004842006701000000204200680200000004000000010000000042006902000000040
 0000000000000042008F0900000008000000004AC0732242000D0200000004000000010000000042000F010000005842

	<pre>005A0500000004000000140000000042007C05000000040000000000000004200790100000030420091070000002437356461396263392D373836372D343963352D383836642D37353766336435323364336600000000</pre>
4	<p>Locate In: uuidKey</p> <p>Tag: Request Message (0x420075), Type: Structure (0x01), Data: Tag: Request Header (0x420074), 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: 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: Request Payload (0x420076), 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: 75da9bc9-7867-49c5-886d-757f3d523d3f</p> <pre>42007501000000B842007401000000384200670100000020420068020000000400000001000000004200690200000004000000000000042000D0200000004000000010000000042000F010000007042005A0500000004000000080000000004200760100000058420008010000005042000A0700000011556E69717565204964656E74696666965720000000000000004200B070000002437356461396263392D373836372D343963352D383836642D37353766336435323364336600000000</pre> <p>Out: <empty response payload></p> <p>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</p> <pre>420078010000008042007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000042008F0900000008000000004AC0732342000D0200000004000000010000000042000F010000002842005A0500000004000000080000000042007C05000000040000000000000004200790100000000</pre>

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

This use-case has two clients performing operations on the same key. The first client initially registers a template and creates a symmetric key using that template. The second client then does a batched Locate and Get using the ID Placeholder to retrieve the key. The second client thereafter performs a number of operations on the key (Get Attribute List, Get Attribute, Add Attribute, Modify Attribute and Delete

Attribute), before the first client finally destroys the key and the template. The first client also tries to Get the key and the template after they have been destroyed, but the Get operation fails in both cases.

This use-case demonstrates the fact that it is possible for two clients to cooperate and use the same managed object while only having knowledge of a single pre-agreed Name attribute value and without having to share any other information. Here, the identities of the two clients are not considered and since we do not include an Authentication field in the header, they could also be considered to be the same client. If the clients authenticate themselves to the server using different credentials, the server needs to employ another policy than the Default policy defined in the KMIP specification on the key object to allow both clients to access it.

Time	Request/Response messages
0	<p>Client A: Register (template) In: objectType='00000007', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', Name={ NameValue='Template1', NameType='00000001' },}</p> <p>Tag: Request Message (0x420075), Type: Structure (0x01), Data: Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000003 (Register) Tag: Request Payload (0x420076), Type: Structure (0x01), Data: Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000006 (Template) Tag: Template-Attribute (0x42008E), 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 (0x420053), Type: Text String (0x07), Data: Template1 Tag: Name Type (0x420052), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)</p> <pre>42007501000001304200740100000038420067010000002042006802000000400000001000000042006902000000040 000000000000042000D02000000400000001000000042000F01000000E842005A050000004000000030000000042 007601000000D0420055050000004000000060000000042008E01000000B8420008010000003042000A0700000017437 27970746F6772617068696320416C676F726974686D0042000B05000000400000003000000042000801000000304200 0A070000001443727970746F67726170686963204C656E677468000000042000B02000000400000080000000042000 8010000004042000A07000000044E616D65000000042000B0100000028420053070000000954656D706C617465310000 00000000042005205000000040000000100000000</pre> <p>Out: uuidTemplate</p>

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: 0x00000003 (Register)
 - Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 - Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 8383198b-4600-4388-955f-2802cc699e9c

42007801000000B0420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042008F0900000008000000004AC0732342000D0200000004000000010000000042000F010000005842005A0500000004000000030000000042007C050000000400000000000000004200790100000003042009107000000243833833313938622D343630302D343338382D393535662D32383032636336393965396300000000

1

Client A:
Create (symmetric key using template)
 In: objectType='00000002', template={ NameValue= 'Template1', NameType='00000001' }, attributes={ Name={ Name='Key1', NameType='00000001' }, CryptographicUsageMask='00000004', ContactInformation='Foo' }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:

- Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000001 (Create)
 - Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 - Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 - Tag: Template-Attribute (0x42008E), Type: Structure (0x01), Data:
 - Tag: Name (0x420051), Type: Structure (0x01), Data:
 - Tag: Name Value (0x420053), Type: Text String (0x07), Data: Template1
 - Tag: Name Type (0x420052), 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 (0x420053), Type: Text String (0x07), Data: Key1
 - Tag: Name Type (0x420052), 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

```
420075010000015842007401000000384200670100000020420068020000004000000010000000042006902000000040
0000000000000042000D020000004000000010000000042000F010000011042005A0500000004000000010000000042
007601000000F84200550500000004000000020000000042008E01000000E042005101000000284200530700000009546
56D706C61746531000000000000042005205000000040000000100000000420008010000003842000A07000000044E61
6D650000000042000B010000002042005307000000044B657931000000004200520500000004000000010000000042000
8010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000
0400000000420008010000003042000A0700000013436F6E7461637420496E666F726D6174696F6E00000000042000B0
700000003466F6F0000000000
```

Out: objectType='00000002', uuidKey

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: 0x000000004AC07324 (Mon Sep 28 10:26:12 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: 0x00000001 (Create)
Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d

```
42007801000000C042007701000000484200670100000020420068020000004000000010000000042006902000000040
0000000000000042008F0900000008000000004AC0732442000D0200000004000000010000000042000F010000006842
005A05000000040000000010000000042007C050000000400000000000000042007901000000404200550500000004000
0000200000000420091070000002437666261303834392D613363322D346438632D383164642D39613139393934376534
376400000000
```

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 (0x420075), Type: Structure (0x01), Data:
Tag: Request Header (0x420074), 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: 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 (0x42005A), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 01F76942FF5A7A8A
 Tag: Request Payload (0x420076), 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 (0x420053), Type: Text String (0x07), Data: Key1
 Tag: Name Type (0x420052), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 3192EDD439D59CC4
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data: null

4200750100000120420074010000004842006701000000204200680200000004000000010000000042006902000000040
 00000000000000420010060000000800000000000000142000D0200000004000000020000000042000F010000009842
 005A050000000400000008000000000420090080000000801F76942FF5A7A8A420076010000000704200080100000028420
 00A070000000B4F626A656374205479706500000000042000B0500000004000000020000000042000801000000384200
 0A07000000044E616D650000000042000B010000002042005307000000044B65793100000000420052050000000400000
 0010000000042000F010000002842005A05000000040000000A0000000042009008000000083192EDD439D59CC4420076
 0100000000

Out: uuidKey
Out: objectType='00000002', uuidKey, symmetricKey

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: 0x000000004AC07324 (Mon Sep 28 10:26:12 CEST 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
 Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 01F76942FF5A7A8A
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 3192EDD439D59CC4
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
 Tag: Symmetric Key (0x42008C), Type: Structure (0x01), Data:

Tag: Key Block (0x42003E), Type: Structure (0x01), Data:
 Tag: Key Format Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001
 Tag: Key Value (0x420043), Type: Structure (0x01), Data:
 Tag: Key Material (0x420041), Type: Octet String (0x08), Data:
 5C7B76DC93EF45FD9231522EB2CE7B0A
 Tag: Cryptographic Algorithm (0x420026), Type: Enumeration (0x05), Data: 0x00000003
 (AES)
 Tag: Cryptographic Length (0x420028), Type: Integer (0x02), Data: 0x00000080 (128)

42007801000001A0420077010000004842006701000000204200680200000004000000010000000042006902000000040
 0000000000000042008F0900000008000000004AC0732442000D0200000004000000020000000042000F010000006842
 005A05000000040000000800000000420090080000000801F76942FF5A7A8A42007C0500000004000000000000000420
 0790100000030420091070000002437666261303834392D613363322D346438632D383164642D39613139393934376534
 37640000000042000F01000000D842005A05000000040000000A0000000042009008000000083192EDD439D59CC442007
 C050000000400000000000000042007901000000A0420055050000000400000002000000004200910700000024376662
 61303834392D613363322D346438632D383164642D3961313939393437653437640000000042008C010000005842003E0
 10000005042004005000000040000000100000000420043010000001842004108000000105C7B76DC93EF45FD9231522E
 B2CE7B0A4200260500000004000000030000000042002802000000040000000800000000

3

Client B:
Get attribute list
In: uuidKey

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d

4200750100000090420074010000003842006701000000204200680200000004000000010000000042006902000000040
 0000000000000042000D0200000004000000010000000042000F010000004842005A05000000040000000C0000000042
 00760100000030420091070000002437666261303834392D613363322D346438632D383164642D3961313939393437653
 43764000000000

Out: uuidKey, attributes={ * }

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: 0x000000004AC07325 (Mon Sep 28 10:26:13 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: 0x0000000C (Get Attribute List)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x420079), Type: Structure (0x01), Data:

- Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
- 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 Changed Date

```
42007801000001D0420077010000004842006701000000204200680200000004000000010000000042006902000000040
0000000000000042008F0900000008000000004AC0732542000D0200000004000000010000000042000F010000017842
005A05000000040000000C0000000042007C050000000400000000000000000000042007901000001504200910700000024376
66261303834392D613363322D346438632D383164642D3961313939393437653437640000000042000A07000000144372
7970746F67726170686963204C656E6774680000000042000A070000001743727970746F6772617068696320416C676F7
26974686D0042000A0700000005537461746500000042000A0700000006446967657374000042000A070000000C496E69
7469616C20446174650000000042000A0700000011556E69717565204964656E7469666965720000000000000042000A0
7000000044E616D650000000042000A070000001843727970746F67726170686963205573616765204D61736B42000A07
0000000B4F626A6563742054797065000000000042000A0700000013436F6E7461637420496E666F726D6174696F6E000
000000042000A07000000114C617374204368616E67656420446174650000000000000000
```

4

Client B:
Get attributes
In: uuidKey, attributeNames={'Name', 'ContactInformation'}

Tag: Request Message (0x420075), Type: Structure (0x01), Data:

- Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
 - Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
 - Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
 - Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information

```
42007501000000C0420074010000003842006701000000204200680200000004000000010000000042006902000000040
0000000000000042000D0200000004000000010000000042000F010000007842005A05000000040000000B0000000042
00760100000060420091070000002437666261303834392D613363322D346438632D383164642D3961313939393437653
437640000000042000A0700000044E616D650000000042000A0700000013436F6E7461637420496E666F726D6174696F
6E000000000000
```

Out: uuidKey, attributes={ Name={ Name='Key1', NameType='00000001' }, ContactInformation='Foo' }

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: 0x000000004AC07325 (Mon Sep 28 10:26:13 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: 0x0000000B (Get Attributes)
 - Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 - Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
 - 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 (0x420053), Type: Text String (0x07), Data: Key1
 - Tag: Name Type (0x420052), 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

420078010000012842007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000042008F0900000008000000004AC0732542000D0200000004000000010000000042000F01000000D042005A05000000040000000B0000000042007C05000000040000000000000042007901000000A8420091070000002437666261303834392D613363322D346438632D383164642D39613139393934376534376400000000420008010000003842000A07000000044E616D650000000042000B010000002042005307000000044B657931000000004200520500000004000000100000000420008010000003042000A0700000013436F6E7461637420496E666F726D6174696F6E000000000042000B0700000003466F6F0000000000

5

Client B:

Add attribute [batch]

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

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

Tag: Request Message (0x420075), Type: Structure (0x01), Data:

- Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 - Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 290C75CAE59F3908
 - Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
 - 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 (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: BF48C307C95CC22E
Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
 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

4200750100000160420074010000003842006701000000204200680200000004000000010000000042006902000000040000000000000042000D02000000040000000020000000042000F010000008842005A05000000040000000D000000004200900800000008290C75CAE59F39084200760100000060420091070000002437666261303834392D613363322D346438632D383164642D39613139393934376534376400000000420008010000002842000A070000000C782D617474726962757465310000000042000B070000000656616C756531000042000F010000008842005A05000000040000000D000000004200900800000008BF48C307C95CC22E4200760100000060420091070000002437666261303834392D613363322D346438632D383164642D39613139393934376534376400000000420008010000002842000A070000000C782D617474726962757465320000000042000B070000000656616C7565320000

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

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

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: 0x000000004AC07326 (Mon Sep 28 10:26:14 CEST 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 290C75CAE59F3908
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
 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 (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: BF48C307C95CC22E
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
 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

4200780100000190420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042000F0900000008000000004AC0732642000D0200000004000000020000000042000F010000009842005A05000000040000000D000000004200900800000008290C75CAE59F390842007C05000000040000000000000000420

0790100000060420091070000002437666261303834392D613363322D346438632D383164642D39613139393934376534
376400000000420008010000002842000A0700000000C782D617474726962757465310000000042000B070000000656616
C756531000042000F010000009842005A05000000040000000D00000000420090080000008BF48C307C95CC22E42007C
05000000040000000000000004200790100000060420091070000002437666261303834392D613363322D346438632D3
83164642D3961313939393437653437640000000420008010000002842000A070000000C782D61747472696275746532
0000000042000B070000000656616C7565320000

6 Client B:
Modify attribute [batch]
In: uuidKey, attribute={ x-attribute1='ModifiedValue1' }
In: uuidKey, attribute={ x-attribute2='ModifiedValue2' }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 42C6D3ED5BFE4F34
Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
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 (0x42005A), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: A391110F7716FCFD
Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
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

42007501000001704200740100000038420067010000002042006802000000400000001000000042006902000000040
0000000000000042000D02000000400000002000000042000F010000009042005A0500000004000000E0000000042
0090080000000842C6D3ED5BFE4F344200760100000068420091070000002437666261303834392D613363322D3464386
32D383164642D3961313939393437653437640000000420008010000003042000A070000000C782D6174747269627574
65310000000042000B070000000E4D6F64696669656456616C756531000042000F010000009042005A05000000040000
00E0000000042009080000008A391110F7716FCFD4200760100000068420091070000002437666261303834392D6133
63322D346438632D383164642D3961313939393437653437640000000420008010000003042000A070000000C782D617
47472696275746532000000042000B070000000E4D6F64696669656456616C7565320000

Out: uuidKey, attribute={ x-ttribute1='ModifiedValue1' }
Out: uuidKey, attribute={ x-attribute2='ModifiedValue2' }

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: 0x000000004AC07326 (Mon Sep 28 10:26:14 CEST 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
 Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 42C6D3ED5BFE4F34
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
 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 (0x42005A), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
 Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: A391110F7716FCFD
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
 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

42007801000001A042007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000042008F0900000008000000004AC0732642000D020000000400000002000000004200F01000000A042005A05000000040000000E00000000420090080000000842C6D3ED5BFE4F3442007C0500000004000000000000004200790100000068420091070000002437666261303834392D613363322D346438632D383164642D39613139393934376534376400000000420008010000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F64696669656456616C756531000042000F01000000A042005A05000000040000000E000000004200900800000008A391110F7716FCFD42007C0500000004000000000000004200790100000068420091070000002437666261303834392D613363322D346438632D383164642D3961313939393437653437640000000420008010000003042000A070000000C782D6174726962757465320000000042000B070000000E4D6F64696669656456616C7565320000

7

Client B:
Delete attribute [batch]
In: uuidKey, attributeNames={'x-attribute1'}
In: uuidKey, attributeNames={'x-attribute2'}

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
 Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: FB10B7D6A5F8F02F
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d

Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 3B5C2DE222A01A87
Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2

4200750100000130420074010000003842006701000000204200680200000004000000010000000042006902000000040
00000000000000042000D0200000004000000020000000042000F010000007042005A05000000040000000F0000000042
00900800000008FB10B7D6A5F8F02F4200760100000048420091070000002437666261303834392D613363322D3464386
32D383164642D3961313939393437653437640000000042000A0700000000C782D61747472696275746531000000004200
0F010000007042005A05000000040000000F0000000042009008000000083B5C2DE222A01A87420076010000004842009
1070000002437666261303834392D613363322D346438632D383164642D3961313939393437653437640000000042000A
070000000C782D6174747269627574653200000000

Out: uuidKey, attributeNames={'x-attribute1'}

Out: uuidKey, attributeNames={'x-attribute2'}

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: 0x000000004AC07327 (Mon Sep 28 10:26:15 CEST 2009)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: FB10B7D6A5F8F02F
Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
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 (0x42005A), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 3B5C2DE222A01A87
Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d
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

42007801000001A0420077010000004842006701000000204200680200000004000000010000000042006902000000040
00000000000000042008F0900000008000000004AC0732742000D0200000004000000020000000042000F01000000A042
005A05000000040000000F000000004200900800000008FB10B7D6A5F8F02F42007C050000000400000000000000420
0790100000068420091070000002437666261303834392D613363322D346438632D383164642D39613139393934376534

	<pre> 376400000000420008010000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F6 4696669656456616C756531000042000F01000000A042005A05000000040000000F0000000042009008000000083B5C2D E22A01A8742007C0500000004000000000000004200790100000068420091070000002437666261303834392D61336 3322D346438632D383164642D39613139393934376534376400000000420008010000003042000A070000000C782D6174 74726962757465320000000042000B070000000E4D6F64696669656456616C7565320000 </pre>
8	<p>Client A: Destroy (symmetric key) In: uuidKey</p> <p>Tag: Request Message (0x420075), Type: Structure (0x01), Data: Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420076), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d</p> <pre> 4200750100000090420074010000003842006701000000204200680200000004000000010000000042006902000000040 0000000000000042000D0200000004000000010000000042000F010000004842005A0500000004000000140000000042 00760100000030420091070000002437666261303834392D613363322D346438632D383164642D3961313939393437653 4376400000000 </pre> <p>Out: uuidKey</p> <p>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: 0x000000004AC07327 (Mon Sep 28 10:26:15 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: 0x00000014 (Destroy) Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d</p> <pre> 42007801000000B0420077010000004842006701000000204200680200000004000000010000000042006902000000040 0000000000000042008F0900000008000000004AC0732742000D0200000004000000010000000042000F010000005842 005A0500000004000000140000000042007C05000000040000000000000042007901000000304200910700000024376 66261303834392D613363322D346438632D383164642D39613139393934376534376400000000 </pre>
9	<p>Client A: Get (symmetric key) In: uuidKey</p>

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8c-81dd-9a199947e47d

420075010000009042007401000000384200670100000020420068020000000400000001000000004200690200000004000000000000042000D0200000004000000010000000042000F010000004842005A05000000040000000A000000004200760100000030420091070000002437666261303834392D613363322D346438632D383164642D39613139393934376534376400000000

Out: Operation Failed, Item Not Found

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: 0x000000004AC07327 (Mon Sep 28 10:26:15 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: 0x0000000A (Get)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000001 (Failed)
 Tag: Result Reason (0x42007B), Type: Enumeration (0x05), Data: 0x00000001 (Item Not Found)
 Tag: Result Message (0x42007A), Type: Text String (0x07), Data: No Cryptographic Object found with given Unique Identifier

42007801000000D042007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000042008F0900000008000000004AC0732742000D0200000004000000010000000042000F010000007842005A05000000040000000A0000000042007C0500000004000000010000000042007B0500000004000000010000000042007A070000003A4E6F2043727970746F67726170686963204F626A65637420666F756E64207769746820676976656E20556E69717565204964656E7469666696572000000000000

10	<p>Client A: Destroy (template) In: uuidTemplate</p> <p>Tag: Request Message (0x420075), Type: Structure (0x01), Data: Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p>
----	--

Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 8383198b-4600-4388-955f-2802cc699e9c

420075010000009042007401000000384200670100000020420068020000000400000001000000004200690200000004000000000000042000D0200000004000000010000000042000F010000004842005A050000000400000014000000004200760100000030420091070000002438333833313938622D343630302D343338382D393535662D32383032636336393965396300000000

Out: uuidTemplate

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: 0x00000004AC07327 (Mon Sep 28 10:26:15 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: 0x00000014 (Destroy)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 8383198b-4600-4388-955f-2802cc699e9c

42007801000000B042007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000042008F0900000008000000004AC0732742000D0200000004000000010000000042000F010000005842005A0500000004000000140000000042007C05000000040000000000000004200790100000030420091070000002438333833313938622D343630302D343338382D393535662D32383032636336393965396300000000

11	<p>Client A: Get (template) In: uuidTemplate</p> <p>Tag: Request Message (0x420075), Type: Structure (0x01), Data: Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420076), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 8383198b-4600-4388-955f-2802cc699e9c</p> <p>420075010000009042007401000000384200670100000020420068020000000400000001000000004200690200000004000000000000042000D0200000004000000010000000042000F010000004842005A05000000040000000A000000004200760100000030420091070000002438333833313938622D343630302D343338382D393535662D32383032636336393965396300000000</p>
----	--

5396300000000

Out: Operation Failed, Item Not Found

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: 0x000000004AC07327 (Mon Sep 28 10:26:15 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: 0x0000000A (Get)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000001 (Failed)
 Tag: Result Reason (0x42007B), Type: Enumeration (0x05), Data: 0x00000001 (Item Not Found)
 Tag: Result Message (0x42007A), Type: Text String (0x07), Data: No Cryptographic Object found with given Unique Identifier

42007801000000D042007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000042008F0900000008000000004AC0732742000D0200000004000000010000000042000F010000007842005A05000000040000000A0000000042007C0500000004000000010000000042007B0500000004000000010000000042007A070000003A4E6F2043727970746F67726170686963204F626A65637420666F756E64207769746820676976656E20556E69717565204964656E746966696572000000000000

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 responses 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='Key1', NameType='00000001' }, CryptographicUsageMask='00000004', ObjectGroup='Group1' }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:

Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000001 (Create)

Tag: Request Payload (0x420076), Type: Structure (0x01), Data:

Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Template-Attribute (0x42008E), 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 (0x420053), Type: Text String (0x07), Data: Key1

Tag: Name Type (0x420052), 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

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

Mask

```
420075010000019042007401000000384200670100000020420068020000000400000001000000042006902000000040
0000000000000042000D020000000400000001000000042000F010000014842005A0500000004000000010000000042
007601000001304200550500000004000000020000000042008E0100000118420008010000003042000A0700000017437
27970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200
0A070000001443727970746F67726170686963204C656E677468000000042000B0200000004000000080000000042000
8010000003842000A07000000044E616D650000000042000B010000002042005307000000044B65793100000000420052
05000000040000000100000000420008010000003042000A070000001843727970746F677261706869632055736167652
04D61736B42000B0200000004000000040000000420008010000002842000A070000000C4F626A6563742047726F7570
0000000042000B070000000647726F7570310000
```

Out: objectType = '00000002', uuidKey

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: 0x000000004AC0781B (Mon Sep 28 10:47:23 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: 0x00000001 (Create)
- Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
- Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 - Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 8b961211-97c7-40a6-8664-ed33491dab5c

42007801000000C0420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042008F0900000008000000004AC0781B42000D020000000400000001000000004200F010000006842005A0500000004000000010000000042007C050000000400000000000000420079010000004042005505000000040000000200000000420091070000002438623936313231312D393763372D343061362D383636342D65643333343931646162356300000000

1

Client B:

Locate (symmetric key by name)

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

Tag: Request Message (0x420075), Type: Structure (0x01), Data:

- Tag: Request Header (0x420074), 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: 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 (0x42005A), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
 - Tag: Request Payload (0x420076), 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 (0x420053), Type: Text String (0x07), Data: Key1
 - Tag: Name Type (0x420052), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007501000000E0420074010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042007060000000800000000000000142000D020000000400000001000000004200F010000008842005A050000000400000008000000004200760100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B05000000040000000200000000420008010000003842000A07000000044E616D6500000004200B010000002042005307000000044B6579310000000042005205000000040000000100000000

Out: asyncCorrValue1

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: 0x000000004AC0781C (Mon Sep 28 10:47:24 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: 0x00000002 (Pending)
 Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: D1DE142AC6367B4B

4200780100000088420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042008F0900000008000000004AC0781C42000D0200000004000000010000000042000F010000003042005A0500000004000000080000000042007C050000000400000002000000004200060800000008D1DE142AC6367B4B

2

Client B:
Poll*
In: asyncCorrValue1

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000001A (Poll)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: D1DE142AC6367B4B

4200750100000070420074010000003842006701000000204200680200000004000000010000000042006902000000040000000000000042000D0200000004000000010000000042000F010000002842005A050000000400000001A0000000042007601000000104200060800000008D1DE142AC6367B4B

Out: uuidKey1

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: 0x000000004AC0781C (Mon Sep 28 10:47:24 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:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 8b961211-97c7-40a6-8664-ed33491dab5c

42007801000000B0420077010000004842006701000000204200680200000004000000010000000042006902000000040

0000000000000042008F0900000008000000004AC0781C42000D0200000004000000010000000042000F010000005842005A0500000004000000080000000042007C05000000040000000000000004200790100000030420091070000002438623936313231312D393763372D343061362D383636342D65643333343931646162356300000000

3

Client B:
Get (symmetric key)
In: uuidKey1

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 8b961211-97c7-40a6-8664-ed33491dab5c

4200750100000090420074010000003842006701000000204200680200000004000000010000000042006902000000040000000000000042000D0200000004000000010000000042000F010000004842005A05000000040000000A000000004200790100000030420091070000002438623936313231312D393763372D343061362D383636342D65643333343931646162356300000000

Out: objectType = '00000002', uuidKey1, symmetricKey

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: 0x00000004AC0781D (Mon Sep 28 10:47:25 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: 0x0000000A (Get)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 8b961211-97c7-40a6-8664-ed33491dab5c
 Tag: Symmetric Key (0x42008C), Type: Structure (0x01), Data:
 Tag: Key Block (0x42003E), Type: Structure (0x01), Data:
 Tag: Key Format Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001
 Tag: Key Value (0x420043), Type: Structure (0x01), Data:
 Tag: Key Material (0x420041), Type: Octet String (0x08), Data: A1DF7B733D8DF7056623FE2D880EF62C
 Tag: Cryptographic Algorithm (0x420026), Type: Enumeration (0x05), Data: 0x00000003 (AES)
 Tag: Cryptographic Length (0x420028), Type: Integer (0x02), Data: 0x00000080 (128)

42007801000001204200770100000048420067010000002042006802000000400000001000000004200690200000040
0000000000000042008F0900000008000000004AC0781D42000D0200000004000000010000000042000F01000000C842
005A05000000040000000A0000000042007C0500000004000000000000000042007901000000A04200550500000004000
0000200000000420091070000002438623936313231312D393763372D343061362D383636342D6564333343931646162
35630000000042008C010000005842003E010000005042004005000000040000000100000000420043010000001842004
10800000010A1DF7B733D8DF7056623FE2D880EF62C420026050000000400000003000000004200280200000004000000
8000000000

4

Client B:
Locate (symmetric key by group)
In: asynchronousIndicator='TRUE', attributes={ objectType = '0000002', ObjectGroup='Group1' }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: 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 (0x42005A), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
 Tag: Request Payload (0x420076), 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

42007501000000D042007401000000484200670100000020420068020000004000000010000000042006902000000040
00000000000000420007060000000800000000000000142000D0200000004000000010000000042000F010000007842
005A050000000400000008000000004200760100000060420008010000002842000A070000000B4F626A6563742054797
06500000000042000B05000000040000000200000000420008010000002842000A070000000C4F626A6563742047726F
75700000000042000B070000000647726F7570310000

Out: asyncCorrValue2

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: 0x000000004AC0781D (Mon Sep 28
10:47:25 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: 0x00000002 (Pending)
 Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:
2DCF4F694617FC30

420078010000008842007701000000484200670100000020420068020000004000000010000000042006902000000040

0000000000000042008F09000000800000004AC0781D4200D020000004000000100000004200F010000003042005A0500000004000000080000000042007C05000000400000002000000042000608000000082DCF4F694617FC30

5
Client B:
Poll*
In: asyncCorrValue2

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000001A (Poll)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:
 2DCF4F694617FC30

42007501000000704200740100000038420067010000002042006802000000400000001000000004200690200000004000000000000042000D0200000004000000010000000042000F010000002842005A05000000040000001A00000000420076010000001042000608000000082DCF4F694617FC30

Out: uuidKey2

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: 0x000000004AC0781D (Mon Sep 28 10:47:25 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:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 8b961211-97c7-40a6-8664-ed33491dab5c

42007801000000B04200770100000048420067010000002042006802000000400000001000000004200690200000004000000000000042008F09000000800000004AC0781D4200D0200000040000001000000004200F010000005842005A0500000004000000080000000042007C05000000400000000000000042007901000000304200910700000002438623936313231312D393763372D343061362D383636342D65643333343931646162356300000000

6
Client B:
Get (symmetric key)
In: uuidKey2

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 8b961211-97c7-40a6-8664-ed33491dab5c

```
4200750100000090420074010000003842006701000000204200680200000040000000100000004200690200000040
000000000000042000D0200000004000000010000000042000F010000004842005A05000000040000000A0000000042
00760100000030420091070000002438623936313231312D393763372D343061362D383636342D6564333334393164616
2356300000000
```

Out: objectType = '00000002', uuidKey2, symmetricKey

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: 0x000000004AC0781D (Mon Sep 28 10:47:25 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: 0x0000000A (Get)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 8b961211-97c7-40a6-8664-ed33491dab5c
 Tag: Symmetric Key (0x42008C), Type: Structure (0x01), Data:
 Tag: Key Block (0x42003E), Type: Structure (0x01), Data:
 Tag: Key Format Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001
 Tag: Key Value (0x420043), Type: Structure (0x01), Data:
 Tag: Key Material (0x420041), Type: Octet String (0x08), Data:
 A1DF7B733D8DF7056623FE2D880EF62C
 Tag: Cryptographic Algorithm (0x420026), Type: Enumeration (0x05), Data: 0x00000003 (AES)
 Tag: Cryptographic Length (0x420028), Type: Integer (0x02), Data: 0x00000080 (128)

```
4200780100000120420077010000004842006701000000204200680200000040000000100000004200690200000040
000000000000042008F0900000008000000004AC0781D42000D0200000004000000010000000042000F01000000C842
005A05000000040000000A0000000042007C05000000040000000000000042007901000000A04200550500000004000
0000200000000420091070000002438623936313231312D393763372D343061362D383636342D65643333343931646162
35630000000042008C010000005842003E010000005042004005000000040000000100000000420043010000001842004
10800000010A1DF7B733D8DF7056623FE2D880EF62C420026050000000400000003000000004200280200000004000000
8000000000
```

7	<p>Client B: Locate (symmetric key by name) In: asynchronousIndicator='TRUE', attributes={ objectType = '00000002', Name= { Name='Key1',</p>
---	--

NameType='00000001' } }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
Tag: Request Header (0x420074), 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: 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 (0x42005A), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
Tag: Request Payload (0x420076), 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 (0x420053), Type: Text String (0x07), Data: Key1
Tag: Name Type (0x420052), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007501000000E0420074010000004842006701000000204200680200000040000000100000000420069020000000400000000000042000706000000800000000000000142000D02000000400000001000000042000F010000008842005A050000000400000008000000004200760100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000020000000420008010000003842000A07000000044E616D65000000042000B010000002042005307000000044B6579310000000042005205000000040000000100000000

Out: asyncCorrValue5

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: 0x000000004AC0781E (Mon Sep 28 10:47:26 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: 0x00000002 (Pending)
Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: D48BDD01A8FFEC80

420078010000008842007701000000484200670100000020420068020000004000000010000000420069020000000400000000000042008F090000000800000004AC0781E42000D02000000400000001000000042000F010000003042005A0500000004000000080000000042007C050000000400000002000000004200060800000008D48BDD01A8FFEC80

8 Client B:
Cancel

In: asyncCorrValue5

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000019 (Cancel)
Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:
D48BDD01A8FFEC80

4200750100000070420074010000003842006701000000204200680200000040000000100000004200690200000040
0000000000000042000D02000000400000001000000042000F010000002842005A050000004000000190000000042
007601000000104200060800000008D48BDD01A8FFEC80

Out: asyncCorrValue5, CancelResult='00000001'

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: 0x000000004AC0781F (Mon Sep 28
10:47:27 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: 0x00000019 (Cancel)
Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:
D48BDD01A8FFEC80
Tag: Cancellation Result (0x420012), Type: Enumeration (0x05), Data: 0x00000001 (Cancelled)

42007801000000A0420077010000004842006701000000204200680200000040000000100000004200690200000040
0000000000000042008F0900000008000000004AC0781F42000D02000000400000001000000042000F010000004842
005A05000000400000019000000042007C05000000400000000000000042007901000000204200060800000008D48
BDD01A8FFEC8042001205000000040000000100000000

9

Client A:
Destroy (symmetric key)
In: uuidKey

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

```

Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
  Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
  Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
    Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 8b961211-97c7-40a6-8664-ed33491dab5c

4200750100000090420074010000003842006701000000204200680200000004000000010000000042006902000000040
0000000000000042000D0200000004000000010000000042000F010000004842005A0500000004000000140000000042
00760100000030420091070000002438623936313231312D393763372D343061362D383636342D6564333334393164616
2356300000000

```

Out: uuidKey

```

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: 0x00000004AC0781F (Mon Sep 28
10:47:27 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: 0x00000014 (Destroy)
    Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 8b961211-97c7-40a6-8664-ed33491dab5c

42007801000000B0420077010000004842006701000000204200680200000004000000010000000042006902000000040
0000000000000042008F0900000008000000004AC0781F42000D0200000004000000010000000042000F010000005842
005A0500000004000000140000000042007C050000000400000000000000042007901000000304200910700000024386
23936313231312D393763372D343061362D383636342D65643333343931646162356300000000

```

* = executed until response is ready

4 Key life cycle support

4.1 Use-case: Revoke scenario

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

Time	Client A
------	----------

0

Client A:

Create (symmetric key)

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

```

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
  Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
      Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x42008E), 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 (0x420053), Type: Text String (0x07), Data: Key1
            Tag: Name Type (0x420052), 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)

```

```

42007501000000160420074010000000384200670100000002042006802000000040000000010000000042006902000000040
0000000000000042000D0200000004000000010000000042000F010000011842005A0500000004000000010000000042
007601000001004200550500000004000000020000000042008E01000000E8420008010000003042000A0700000017437
27970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200
0A070000001443727970746F67726170686963204C656E677468000000042000B02000000040000000800000000042000
8010000003842000A07000000044E616D650000000042000B010000002042005307000000044B65793100000000420052
050000000400000001000000004200080100000003042000A0700000001843727970746F677261706869632055736167652
04D61736B42000B02000000040000000400000000

```

Out: objectType = '00000002', uuidKey

```

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: 0x000000004AC0781F (Mon Sep 28
10:47:27 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: 0x00000001 (Create)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

 42007801000000C0420077010000004842006701000000204200680200000004000000010000000042006902000000040
 000000000000000042008F0900000008000000004AC0781F42000D0200000004000000010000000042000F010000006842
 005A0500000004000000010000000042007C05000000040000000000000042007901000000404200550500000004000
 0000200000000420091070000002433333364633962392D386537332D346666362D613337622D34323336396635613432
 363200000000

1
Client A:
Get attribute
In: uuidKey, attributeName={'State'}

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

 42007501000000A0420074010000003842006701000000204200680200000004000000010000000042006902000000040
 000000000000000042000D0200000004000000010000000042000F010000005842005A05000000040000000B0000000042
 007601000000040420091070000002433333364633962392D386537332D346666362D613337622D3432333639663561343
 236320000000042000A07000000055374617465000000

Out: uuidKey, attribute={ State='00000001' }

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: 0x000000004AC07820 (Mon Sep 28 10:47:28 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: 0x0000000B (Get Attributes)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-

42369f5a4262

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)

42007801000000D8420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042008F0900000008000000004AC0782042000D0200000004000000010000000042000F010000008042005A05000000040000000B0000000042007C0500000004000000000000000420079010000005842009107000000243333364633962392D386537332D346666362D613337622D34323336396635613432363200000000420008010000002042000A0700000005537461746500000042000B05000000040000000100000000

2

Client A:
Add attribute
In: uuidKey, attribute={ ActivationDate='2' }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262
 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 1970)

42007501000000C0420074010000003842006701000000204200680200000004000000010000000042006902000000040000000000000042000D0200000004000000010000000042000F010000007842005A05000000040000000D00000000420076010000006042009107000000243333364633962392D386537332D346666362D613337622D34323336396635613432363200000000420008010000002842000A07000000F41637469766174696F6E20446174650042000B090000000800000000000000

Out: uuidKey, attribute={ ActivationDate='2' }

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: 0x000000004AC07820 (Mon Sep 28 10:47:28 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: 0x0000000D (Add Attribute)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-

42369f5a4262

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 1970)

42007801000000E042007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000042008F0900000008000000004AC0782042000D0200000004000000010000000042000F010000008842005A05000000040000000D0000000042007C0500000004000000000000000420079010000006042009107000000243333364633962392D386537332D346666362D613337622D343233363966356134323632000000042000801000000284200A070000000F41637469766174696F6E20446174650042000B09000000080000000000000002

3

Client A:

Get attribute

In: uuidKey, attributeName={ 'State' }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:

Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)

Tag: Request Payload (0x420076), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

42007501000000A042007401000000384200670100000020420068020000000400000001000000004200690200000004000000000000042008F0900000008000000004AC0782042000D0200000004000000010000000042000F010000005842005A05000000040000000B0000000042007C05000000040000000D00000000420079010000006042009107000000243333364633962392D386537332D346666362D613337622D343233363966356134323632000000042000A07000000055374617465000000

Out: uuidKey, attribute={ State='0000002' }

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: 0x000000004AC07820 (Mon Sep 28 10:47:28 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: 0x0000000B (Get Attributes)

Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

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)

42007801000000D842007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000042008F0900000008000000004AC0782042000D0200000004000000010000000042000F010000008042005A050000000400000000B0000000042007C0500000004000000000000000420079010000005842009107000000243333364633962392D386537332D346666362D613337622D3432333639663561343236320000000042000801000000204200A0700000005537461746500000042000B05000000040000000200000000

4

Client B:
Locate (symmetric key by name)
In: objectType = '00000002', attributes={ Name={ Name='Key1', NameType='00000001' } }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
Tag: Request Header (0x420074), 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: 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: Request Payload (0x420076), 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 (0x420053), Type: Text String (0x07), Data: Key1
Tag: Name Type (0x420052), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007501000000D042007401000000384200670100000020420068020000000400000001000000004200690200000004000000000000042000D0200000004000000010000000042000F010000008042005A0500000004000000080000000004200760100000070420008010000002842000A0700000000B4F626A656374205479706500000000042000B05000000040000000000000420008010000003842000A07000000044E616D650000000042000B010000002042005307000000044B6579310000000042005205000000040000000100000000

Out: uuidKey

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: 0x000000004AC07821 (Mon Sep 28 10:47:29 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:

Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

42007801000000B0420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042008F0900000008000000004AC0782142000D0200000004000000010000000042000F010000005842005A0500000004000000080000000042007C05000000040000000000000000420079010000003042009107000000243333364633962392D386537332D346666362D613337622D3432333639635613432363200000000

5

Client B:
Get (symmetric key)
In: uuidKey

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

4200750100000090420074010000003842006701000000204200680200000004000000010000000042006902000000040000000000000042000D0200000004000000010000000042000F010000004842005A05000000040000000A00000000420076010000003042009107000000243333364633962392D386537332D346666362D613337622D3432333639635613432363200000000

Out: objectType = '00000002', uuidKey, symmetricKey

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: 0x000000004AC07821 (Mon Sep 28 10:47:29 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: 0x0000000A (Get)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262
 Tag: Symmetric Key (0x42008C), Type: Structure (0x01), Data:
 Tag: Key Block (0x42003E), Type: Structure (0x01), Data:
 Tag: Key Format Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001
 Tag: Key Value (0x420043), Type: Structure (0x01), Data:
 Tag: Key Material (0x420041), Type: Octet String (0x08), Data: E6C15B28BB6C7A268E9ADEA471A36F23

Tag: Cryptographic Algorithm (0x420026), Type: Enumeration (0x05), Data: 0x00000003 (AES)

Tag: Cryptographic Length (0x420028), Type: Integer (0x02), Data: 0x00000080 (128)

4200780100000120420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042008F0900000008000000004AC0782142000D0200000004000000010000000042000F01000000C842005A05000000040000000A0000000042007C050000000400000000000000042007901000000A0420055050000000400000000200091070000002433333364633962392D386537332D3466666362D613337622D3432333639663561343236320000000042008C010000005842003E01000000504200400500000004000000010000000042004301000000184200410800000010E6C15B28BB6C7A268E9ADEA471A36F234200260500000004000000030000000042002802000000040000008000000000

6

Client B:

Revoke (symmetric key as compromised)

In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceTime='6'

Tag: Request Message (0x420075), Type: Structure (0x01), Data:

Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)

Tag: Request Payload (0x420076), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

Tag: Revocation Reason (0x42007E), Type: Structure (0x01), Data:

Tag: Revocation Reason Code (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Key Compromise)

Tag: Compromise Occurrence Date (0x42001F), Type: Date-Time (0x09), Data: 0x0000000000000006 (Thu Jan 01 01:00:06 CET 1970)

42007501000000B8420074010000003842006701000000204200680200000004000000010000000042006902000000040000000000000042008D0200000004000000010000000042000F010000007042005A050000000400000013000000004200760100000058420091070000002433333364633962392D386537332D3466666362D613337622D3432333639663561343236320000000042007E010000001042007F0500000004000000020000000042001F09000000080000000000000006

Out: uuidKey

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: 0x000000004AC07822 (Mon Sep 28 10:47:30 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: 0x00000013 (Revoke)

Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-

42369f5a4262

42007801000000B042007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000042008F0900000008000000004AC0782242000D0200000004000000010000000042000F010000005842005A0500000004000000130000000042007C0500000004000000000000000420079010000003042009107000000243333364633962392D386537332D346666362D613337622D34323336396635613432363200000000

7

Client B:
Get attribute
In: uuidKey, attributeName={ 'State' }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

42007501000000A042007401000000384200670100000020420068020000000400000001000000004200690200000004000000000000042000D0200000004000000010000000042000F010000005842005A05000000040000000B0000000004200760100000004042009107000000243333364633962392D386537332D346666362D613337622D3432333639663561343236320000000042000A07000000055374617465000000

Out: uuidKey, attribute={ State='00000004' }

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: 0x00000004AC07822 (Mon Sep 28 10:47:30 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: 0x0000000B (Get Attributes)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262
 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)

42007801000000D842007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000042008F0900000008000000004AC0782242000D0200000004000000010000000042000F0100000008042005A05000000040000000B0000000042007C050000000400000000000000042007901000000584200910700000024333

33364633962392D386537332D346666362D613337622D343233363966356134323632000000042000801000000204200A0700000005537461746500000042000B05000000040000000400000000

8

Client A:
Get attribute list
In: uuidKey

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

420075010000009042007401000000384200670100000020420068020000000400000001000000004200690200000004000000000000042000D0200000004000000010000000042000F010000004842005A05000000040000000C000000004200760100000030420091070000002433333364633962392D386537332D346666362D613337622D34323336396635613432363200000000

Out: uuidKey, attributes = { * }

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: 0x000000004AC07822 (Mon Sep 28 10:47:30 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: 0x0000000C (Get Attribute List)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262
 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 Changed Date

42007801000002284200770100000048420067010000002042006802000000400000001000000042006902000000040
0000000000000042008F090000000800000004AC0782242000D0200000040000000100000004200F01000001D042
005A05000000040000000C0000000042007C05000000040000000000000042007901000001A84200910700000024333
33364633962392D386537332D346666362D613337622D343233363966356134323632000000042000A07000000144372
7970746F67726170686963204C656E677468000000042000A070000001743727970746F6772617068696320416C676F7
26974686D0042000A0700000005537461746500000042000A070000001A436F6D70726F6D69736520446174650042000A0700000064469676
636520446174650000000000042000A07000000F436F6D70726F6D69736520446174650042000A0700000064469676
57374000042000A07000000C496E697469616C2044617465000000042000A07000000F41637469766174696F6E2044
6174650042000A07000000115265766F636174696F6E20526561736F6E000000000000042000A0700000011556E69717
565204964656E746966696572000000000000042000A0700000044E616D650000000042000A07000000184372797074
6F67726170686963205573616765204D61736B42000A07000000B4F626A656374205479706500000000042000A07000
000114C617374204368616E676564204461746500000000000000

9

Client A:

Get attributes

In: uuidKey, attributeName = { 'State' }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:

Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)

Tag: Request Payload (0x420076), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

42007501000000A04200740100000038420067010000002042006802000000400000001000000042006902000000040
0000000000000042000D0200000004000000010000000042000F010000005842005A05000000040000000B0000000042
0076010000004042009107000000243333364633962392D386537332D346666362D613337622D3432333639663561343
236320000000042000A07000000055374617465000000

Out: uuidKey, attribute={ State='00000004' }

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: 0x000000004AC07822 (Mon Sep 28 10:47:30 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: 0x0000000B (Get Attributes)

Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-

42369f5a4262
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)

42007801000000D8420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042008F0900000008000000004AC0782242000D020000000400000001000000004200F010000008042005A05000000040000000B0000000042007C0500000004000000000000004200790100000058420091070000002433333364633962392D386537332D346666362D613337622D3432333639663561343236320000000042008010000002042000A0700000005537461746500000042000B05000000040000000400000000

10 Client A:
Add attribute [batch]
In: uuidKey, attribute={ x-attribute1='Value1' }
In: uuidKey, attribute={ x-attribute2='Value2' }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 5CD7C98FC5B52FF7
Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262
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 (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: F0CB35D89BB9D251
Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262
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

4200750100000160420074010000003842006701000000204200680200000004000000010000000042006902000000040000000000000042008F010000008842005A05000000040000000D0000000042009008000000085CD7C98FC5B52FF742007601000000060420091070000000243333364633962392D386537332D346666362D613337622D3432333639663561343236320000000042008010000002842000A070000000C782D617474726962757465310000000042000B070000000656616C756531000042000F010000008842005A05000000040000000D000000004200900800000008F0CB35D89BB9D2514200760100000006042009107000000243333364633962392D386537332D346666362D613337622D3432333639663561343236320000000042008010000002842000A070000000C782D61747472696275746532000000042000B070000000656616C7565320000

Out: uuidKey, attribute={ x-attribute1='Value1' }
Out: uuidKey, attribute={ x-attribute2='Value2' }

```

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: 0x000000004AC07823 (Mon Sep 28
10:47:31 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 5CD7C98FC5B52FF7
    Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-
42369f5a4262
      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 (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
      Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: F0CB35D89BB9D251
      Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
      Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
        Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-
42369f5a4262
        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

4200780100000190420077010000004842006701000000204200680200000004000000010000000042006902000000040
000000000000042008F0900000008000000004AC0782342000D0200000004000000020000000042000F010000009842
005A05000000040000000D000000042009008000000085CD7C98FC5B52FF742007C050000000400000000000000420
0790100000060420091070000002433333364633962392D386537332D346666362D613337622D34323336396635613432
363200000000420008010000002842000A070000000C782D617474726962757465310000000042000B070000000656616
C756531000042000F010000009842005A05000000040000000D00000000420090080000008F0CB35D89BB9D25142007C
050000004000000000000004200790100000060420091070000002433333364633962392D386537332D346666362D6
13337622D34323336396635613432363200000000420008010000002842000A070000000C782D61747472696275746532
0000000042000B070000000656616C7565320000

```

11

Client A:
 Modify attribute [batch]
 In: uuidKey, attribute={ x-attribute1='ModifiedValue1' }
 In: uuidKey, attribute={ x-attribute2='ModifiedValue2' }

```

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
  Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

```

Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
 Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: C06597C23C952144
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262
 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 (0x42005A), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
 Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 3D9CF6E0445252B8
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262
 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

4200750100000170420074010000003842006701000000204200680200000004000000010000000042006902000000040
 0000000000000042000D0200000004000000020000000042000F010000009042005A05000000040000000E0000000042
 00900800000008C06597C23C952144420076010000006842009107000000243333364633962392D386537332D3466663
 62D613337622D3432333639663561343236320000000420008010000003042000A070000000C782D6174747269627574
 65310000000042000B070000000E4D6F64696669656456616C756531000042000F010000009042005A05000000040000
 00E0000000042009008000000083D9CF6E0445252B8420076010000006842009107000000243333364633962392D3865
 37332D346666362D613337622D3432333639663561343236320000000420008010000003042000A070000000C782D617
 47472696275746532000000042000B070000000E4D6F64696669656456616C7565320000

Out: uuidKey, attribute={ x-attribute1='ModifiedValue1' }

Out: uuidKey, attribute={ x-attribute2='ModifiedValue2' }

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: 0x00000004AC07823 (Mon Sep 28 10:47:31 CEST 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
 Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: C06597C23C952144
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262
 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 (0x42005A), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
 Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 3D9CF6E0445252B8
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

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

42007801000001A042007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000042008F0900000008000000004AC0782342000D020000000400000002000000042000F01000000A042005A05000000040000000E000000004200900800000008C06597C23C95214442007C0500000004000000000000000420079010000006842009107000000243333364633962392D386537332D346666362D613337622D343233363966356134323632000000042008010000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F64696669656456616C756531000042000F01000000A042005A05000000040000000E0000000042009008000000083D9CF6E0445252B842007C050000000400000000000000420079010000006842009107000000243333364633962392D386537332D346666362D613337622D343233363966356134323632000000042008010000003042000A070000000C782D61747472696275746532000000042000B070000000E4D6F64696669656456616C7565320000

12

Client A:

Delete attribute [batch]

In: uuidKey, attributeNames={ 'x-attribute1' }

In: uuidKey, attributeNames={ 'x-attribute2' }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:

Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)

Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)

Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 1A1B48172DF57ABC

Tag: Request Payload (0x420076), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1

Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)

Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: B77FD0753B7C95ED

Tag: Request Payload (0x420076), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2

420075010000013042007401000000384200670100000020420068020000000400000001000000004200690200000004000000000000042000D0200000004000000020000000042000F010000007042005A05000000040000000F0000000042009008000000081A1B48172DF57ABC420076010000004842009107000000243333364633962392D386537332D346666362D613337622D343233363966356134323632000000042000A070000000C782D617474726962757465310000000042000B070000000E4D6F64696669656456616C756532000000042000F01000000A042005A05000000040000000E0000000042009008000000083D9CF6E0445252B842007C050000000400000000000000420079010000006842009107000000243333364633962392D386537332D346666362D613337622D343233363966356134323632000000042008010000003042000A070000000C782D61747472696275746532000000042000B070000000E4D6F64696669656456616C7565320000

Out: uuidKey, attributeNames={ 'x-attribute1' }

Out: uuidKey, attributeNames={ 'x-attribute2' }

```

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: 0x000000004AC07826 (Mon Sep 28
10:47:34 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
    Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: 1A1B48172DF57ABC
    Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-
42369f5a4262
      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 (0x42005A), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
      Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: B77FD0753B7C95ED
      Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
      Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
        Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-
42369f5a4262
        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

42007801000001A04200770100000048420067010000002042006802000000040000000010000000042006902000000040
000000000000042008F0900000008000000004AC0782642000D0200000004000000020000000042000F01000000A042
005A050000000400000000F0000000042009008000000081A1B48172DF57ABC42007C050000000400000000000000420
07901000000684200910700000002433333364633962392D386537332D346666362D613337622D34323336396635613432
363200000000420008010000003042000A0700000000C782D617474726962757465310000000042000B070000000E4D6F6
4696669656456616C756531000042000F01000000A042005A050000000400000000F000000004200900800000008B77FD0
753B7C95ED42007C05000000040000000000000042007901000000684200910700000002433333364633962392D38653
7332D346666362D613337622D3432333639663561343236320000000420008010000003042000A070000000C782D6174
74726962757465320000000042000B070000000E4D6F64696669656456616C7565320000

```

13

Client A:
Get (symmetric key)
In: uuidKey

```

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
  Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000A (Get)

```

Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

420075010000009042007401000000384200670100000020420068020000000400000001000000004200690200000004000000000000042000D0200000004000000010000000042000F010000004842005A05000000040000000A000000004200760100000030420091070000002433333364633962392D386537332D346666362D613337622D34323336396635613432363200000000

Out: objectType = '00000002', uuidKey, symmetricKey

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: 0x000000004AC07827 (Mon Sep 28 10:47:35 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: 0x0000000A (Get)

Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x420079), Type: Structure (0x01), Data:

Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

Tag: Symmetric Key (0x42008C), Type: Structure (0x01), Data:

Tag: Key Block (0x42003E), Type: Structure (0x01), Data:

Tag: Key Format Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001

Tag: Key Value (0x420043), Type: Structure (0x01), Data:

Tag: Key Material (0x420041), Type: Octet String (0x08), Data: E6C15B28BB6C7A268E9ADEA471A36F23

Tag: Cryptographic Algorithm (0x420026), Type: Enumeration (0x05), Data: 0x00000003 (AES)

Tag: Cryptographic Length (0x420028), Type: Integer (0x02), Data: 0x00000080 (128)

420078010000012042007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000042008F0900000008000000004AC0782742000D0200000004000000010000000042000F01000000C842005A05000000040000000A0000000042007C050000000400000000000000042007901000000A0420055050000000400000000000420091070000002433333364633962392D386537332D346666362D613337622D343233363966356134323632000000042008C010000005842003E01000000504200400500000004000000010000000042004301000000184200410800000010E6C15B28BB6C7A268E9ADEA471A36F234200260500000004000000030000000042002802000000040000008000000000

14

Client A:
Destroy (symmetric key)
In: uuidKey

Tag: Request Message (0x420075), Type: Structure (0x01), Data:

Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

```
4200750100000090420074010000003842006701000000204200680200000004000000010000000042006902000000040
0000000000000042000D0200000004000000010000000042000F010000004842005A0500000004000000140000000042
007601000000304200910700000002433333364633962392D386537332D346666362D613337622D3432333639663561343
2363200000000
```

Out: uuidKey

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: 0x000000004AC07827 (Mon Sep 28 10:47:35 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: 0x00000014 (Destroy)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262

```
42007801000000B0420077010000004842006701000000204200680200000004000000010000000042006902000000040
0000000000000042008F0900000008000000004AC0782742000D0200000004000000010000000042000F010000005842
005A0500000004000000140000000042007C050000000400000000000000042007901000000304200910700000024333
33364633962392D386537332D346666362D613337622D34323336396635613432363200000000
```

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, while a third fails since the usage allocation has been used up. The key is finally 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 (0x420075), Type: Structure (0x01), Data:
Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000001 (Create)
Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
Tag: Template-Attribute (0x42008E), 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 (0x420053), Type: Text String (0x07), Data: Key1
Tag: Name Type (0x420052), 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)

420075010000001604200740100000038420067010000002042006802000000040000000100000000420069020000000400
0000000000000042000D0200000004000000010000000042000F010000011842005A050000000400000001000000004200
7601000001004200550500000004000000020000000042008E01000000E8420008010000003042000A0700000017437279
70746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000A07
0000001443727970746F67726170686963204C656E6774680000000042000B020000000400000008000000004200080100
00003842000A07000000044E616D650000000042000B010000002042005307000000044B65793100000000420052050000
00040000000100000000420008010000003042000A070000001843727970746F67726170686963205573616765204D6173
6B42000B02000000040000000400000000

Out: objectType = '00000002', uuidKey

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: 0x000000004AC07828 (Mon Sep 28 10:47:36 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: 0x00000001 (Create)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615

 420078010000000C04200770100000048420067010000002042006802000000040000000100000000420069020000000400
 0000000000000042008F0900000008000000004AC0782842000D020000000400000001000000004200F01000000684200
 5A0500000004000000010000000042007C050000000400000000000000042007901000000404200550500000004000000
 02000000004200910700000002434666563336135392D623231372D346162662D383461642D616631353437303234363135
 00000000

1
Client A:
Add attribute [batch]
In: uuidKey, attribute={ ActivationDate='2' }
In: uuidKey, attribute={ ProtectStopDate='<NOW+10min>' }

 Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: E1AE8A5206CC749A
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615
 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 1970)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: C6CAA6E0C409336F
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615
 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: 0x000000004AC07A80 (Mon Sep 28 10:57:36 CEST 2009)

 42007501000001684200740100000038420067010000002042006802000000040000000100000000420069020000000400
 0000000000000042000D020000000400000002000000004200F010000008842005A05000000040000000D000000004200
 900800000008E1AE8A5206CC749A4200760100000060420091070000002434666563336135392D623231372D346162662D
 383461642D61663135343730323436313500000000420008010000002842000A070000000F41637469766174696F6E2044
 6174650042000B090000000800000000000000000000242000F010000009042005A05000000040000000D000000004200900800
 000008C6CAA6E0C409336F4200760100000068420091070000002434666563336135392D623231372D346162662D383461
 642D61663135343730323436313500000000420008010000003042000A070000001150726F746563742053746F70204461
 7465000000000000042000B0900000008000000004AC07A80

Out: uuidKey, attribute={ ActivationDate='2' }
Out: uuidKey, attribute={ ProtectStopDate='<NOW+10min>' }

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: 0x000000004AC07828 (Mon Sep 28 10:47:36 CEST 2009)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: E1AE8A5206CC749A
Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615
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 1970)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
Tag: Unique Batch Item ID (0x420090), Type: Octet String (0x08), Data: C6CAA6E0C409336F
Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615
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: 0x000000004AC07A80 (Mon Sep 28 10:57:36 CEST 2009)

42007801000001984200770100000048420067010000002042006802000000040000000100000000420069020000000400
0000000000000042008F0900000008000000004AC0782842000D0200000004000000020000000042000F01000000984200
5A0500000004000000D000000004200900800000008E1AE8A5206CC749A42007C0500000004000000000000000420079
01000000604200910700000002434666563336135392D623231372D346162662D383461642D616631353437303234363135
0000000042008010000002842000A070000000F41637469766174696F6E20446174650042000B09000000080000000000
00000242000F01000000A042005A05000000040000000D000000004200900800000008C6CAA6E0C409336F42007C050000
000400000000000004200790100000068420091070000002434666563336135392D623231372D346162662D38346164
2D6166313534373032343631350000000042008010000003042000A070000001150726F746563742053746F7020446174
65000000000000042000B0900000008000000004AC07A80

2 Client A:
Add Attribute
In: uuidKey, attribute={ UsageLimits={ UsageLimitsTotalBytes='1000' } }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615
 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 Bytes (0x420095), Type: Big Integer (0x04), Data: 03E8 (1000)

420075010000000C84200740100000038420067010000002042006802000000040000000100000000420069020000000400
 000000000000042000D0200000004000000010000000042000F010000008042005A05000000040000000D000000004200
 760100000068420091070000002434666563336135392D623231372D346162662D383461642D6166313534373032343631
 350000000042000801000000304200A070000000C5573616765204C696D697473000000004200B010000001042009504
 000000080000000000000003E8

Out: uuidKey, attribute={ UsageLimits={ UsageLimitsTotalBytes= '1000', UsageLimitsByteCount='1000' } }

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: 0x000000004AC0782A (Mon Sep 28 10:47:38 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: 0x0000000D (Add Attribute)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615
 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 Bytes (0x420095), Type: Big Integer (0x04), Data: 00000000000003E8 (1000)
 Tag: Usage Limits Byte Count (0x420093), Type: Big Integer (0x04), Data: 00000000000003E8 (1000)

42007801000000F84200770100000048420067010000002042006802000000040000000100000000420069020000000400
 0000000000000042008F0900000008000000004AC0782A4200D020000000400000001000000004200F01000000A04200
 5A05000000040000000D0000000042007C05000000040000000000000042007901000000784200910700000024346665
 63336135392D623231372D346162662D383461642D616631353437303234363135000000004200801000000404200A07
 0000000C5573616765204C696D697473000000004200B0100000020420095040000000800000000000003E84200930400
 0000080000000000000003E8

3	<p>Client B: Locate (symmetric key by name) In: objectType = '00000002', attributes={ Name={ Name='Key1', NameType= '00000001' } }</p>
---	---

Tag: Request Message (0x420075), Type: Structure (0x01), Data:

- Tag: Request Header (0x420074), 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: 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: Request Payload (0x420076), 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 (0x420053), Type: Text String (0x07), Data: Key1
 - Tag: Name Type (0x420052), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007501000000D0420074010000003842006701000000204200680200000040000000100000000420069020000000400000000000042000D0200000004000000010000000042000F010000008842005A050000000400000008000000004200760100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B05000000040000000200000000420008010000003842000A07000000044E616D65000000042000B010000002042005307000000044B657931000000042005205000000040000000100000000

Out: uuidKey

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: 0x00000004AC0782A (Mon Sep 28 10:47:38 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:
 - Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615

42007801000000B04200770100000048420067010000002042006802000000400000001000000004200690200000004000000000000042000F0900000008000000004AC0782A42000D0200000004000000010000000042000F010000005842005A0500000004000000080000000042007C05000000040000000000000004200790100000030420091070000002434666563336135392D623231372D346162662D383461642D61663135343730323436313500000000

4 Client B:
Get (symmetric key)
In: uuidKey

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615

42007501000000904200740100000038420067010000002042006802000000400000001000000042006902000000400
 00000000000042000D020000000400000001000000042000F010000004842005A0500000040000000A000000004200
 760100000030420091070000002434666563336135392D623231372D346162662D383461642D6166313534373032343631
 3500000000

Out: objectType = '00000002', uuidKey, symmetricKey

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: 0x00000004AC0782A (Mon Sep 28 10:47:38 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: 0x0000000A (Get)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615
 Tag: Symmetric Key (0x42008C), Type: Structure (0x01), Data:
 Tag: Key Block (0x42003E), Type: Structure (0x01), Data:
 Tag: Key Format Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001
 Tag: Key Value (0x420043), Type: Structure (0x01), Data:
 Tag: Key Material (0x420041), Type: Octet String (0x08), Data:
 3D41DF1C5C20E272212D86D762A8C7D4
 Tag: Cryptographic Algorithm (0x420026), Type: Enumeration (0x05), Data: 0x00000003 (AES)
 Tag: Cryptographic Length (0x420028), Type: Integer (0x02), Data: 0x00000080 (128)

42007801000001204200770100000048420067010000002042006802000000400000001000000042006902000000400
 00000000000042008F090000000800000004AC0782A42000D02000000400000001000000042000F01000000C84200
 5A0500000040000000A0000000042007C050000000400000000000000042007901000000A04200550500000004000000
 0200000000420091070000002434666563336135392D623231372D346162662D383461642D616631353437303234363135
 0000000042008C010000005842003E0100000050420040050000000400000001000000042004301000000184200410800
 0000103D41DF1C5C20E272212D86D762A8C7D4420026050000004000000030000000420028020000004000000800000
 0000

5	Client B:
---	-----------

Get usage allocation

In: uuidKey, UsageLimitsByteCount='500'

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)
Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615
Tag: Usage Limits Byte Count (0x420093), Type: Big Integer (0x04), Data: 01F4 (500)

42007501000000A042007401000000384200670100000020420068020000004000000010000000042006902000000400
00000000000042000D0200000004000000010000000042000F010000005842005A05000000400000011000000004200
760100000040420091070000002434666563336135392D623231372D346162662D383461642D6166313534373032343631
3500000000420093040000000800000000000001F4

Out: uuidKey

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: 0x000000004AC0782A (Mon Sep 28 10:47:38 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: 0x00000011 (Get Usage Allocation)
Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615

42007801000000B042007701000000484200670100000020420068020000004000000010000000042006902000000400
00000000000042008F0900000008000000004AC0782A42000D020000004000000010000000042000F01000000584200
5A0500000004000000110000000042007C0500000004000000000000000042007901000000304200910700000024346665
63336135392D623231372D346162662D383461642D61663135343730323436313500000000

6

Client A:
Get usage allocation
In: uuidKey, UsageLimitsByteCount='500'

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615
 Tag: Usage Limits Byte Count (0x420093), Type: Big Integer (0x04), Data: 01F4 (500)

42007501000000A0420074010000003842006701000000204200680200000040000000100000000420069020000000400
 0000000000000042000D0200000004000000010000000042000F010000005842005A050000000400000011000000004200
 760100000040420091070000002434666563336135392D623231372D346162662D383461642D6166313534373032343631
 35000000004200930400000008000000000000001F4

Out: uuidKey

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: 0x000000004AC0782B (Mon Sep 28 10:47:39 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: 0x00000011 (Get Usage Allocation)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615

42007801000000B0420077010000004842006701000000204200680200000040000000100000000420069020000000400
 0000000000000042008F0900000008000000004AC0782B42000D020000004000000010000000042000F01000000584200
 5A0500000004000000110000000042007C050000000400000000000000042007901000000304200910700000024346665
 63336135392D623231372D346162662D383461642D61663135343730323436313500000000

7 **Client C:**
Locate (symmetric key by name)
In: objectType = '00000002', attributes={ Name={ Name='Key1', NameType='00000001' } }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: 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: Request Payload (0x420076), 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 (0x420053), Type: Text String (0x07), Data: Key1
 Tag: Name Type (0x420052), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007501000000D04200740100000038420067010000002042006802000000040000000100000000420069020000000400
 0000000000000042000D0200000004000000010000000042000F010000008842005A050000000400000008000000004200
 760100000070420008010000002842000A070000000B4F626A6563742054797065000000000042000B0500000004000000
 020000000420008010000003842000A07000000044E616D65000000042000B010000002042005307000000044B657931
 0000000042005205000000040000000100000000

Out: uuidKey

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: 0x000000004AC0782B (Mon Sep 28 10:47:39 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:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615

42007801000000B04200770100000048420067010000002042006802000000040000000100000000420069020000000400
 0000000000000042008F0900000008000000004AC0782B42000D0200000004000000010000000042000F01000000584200
 5A0500000004000000080000000042007C0500000004000000000000000042007901000000304200910700000024346665
 63336135392D623231372D346162662D383461642D61663135343730323436313500000000

8 Client C:
 Get (symmetric key)
 In: uuidKey

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-

af1547024615

420075010000009042007401000000384200670100000020420068020000004000000010000000042006902000000400000000000042000D0200000004000000010000000042000F010000004842005A0500000040000000A000000004200760100000030420091070000002434666563336135392D623231372D346162662D383461642D61663135343730323436313500000000

Out: objectType = '00000002', uuidKey, symmetricKey

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: 0x000000004AC0782B (Mon Sep 28 10:47:39 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: 0x0000000A (Get)

Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x420079), Type: Structure (0x01), Data:

Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615

Tag: Symmetric Key (0x42008C), Type: Structure (0x01), Data:

Tag: Key Block (0x42003E), Type: Structure (0x01), Data:

Tag: Key Format Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001

Tag: Key Value (0x420043), Type: Structure (0x01), Data:

Tag: Key Material (0x420041), Type: Octet String (0x08), Data: 3D41DF1C5C20E272212D86D762A8C7D4

Tag: Cryptographic Algorithm (0x420026), Type: Enumeration (0x05), Data: 0x00000003 (AES)

Tag: Cryptographic Length (0x420028), Type: Integer (0x02), Data: 0x00000080 (128)

420078010000012042007701000000484200670100000020420068020000004000000010000000042006902000000400000000000042008F0900000008000000004AC0782B42000D020000004000000010000000042000F01000000C842005A05000000040000000A0000000042007C05000000040000000000000042007901000000A0420055050000004000000020000000420091070000002434666563336135392D623231372D346162662D383461642D616631353437303234363135000000042008C010000005842003E010000005042004005000000040000000010000000042004301000000184200410800000103D41DF1C5C20E272212D86D762A8C7D4420026050000004000000030000000420028020000004000000800000000

9

Client C:

Get usage allocation

In: uuidKey, UsageLimitsByteCount='500'

Tag: Request Message (0x420075), Type: Structure (0x01), Data:

Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

	<p>Tag: Batch Item (0x4200F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)</p> <p>Tag: Request Payload (0x420076), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615</p> <p>Tag: Usage Limits Byte Count (0x420093), Type: Big Integer (0x04), Data: 01F4 (500)</p> <p>42007501000000A04200740100000038420067010000002042006802000000040000000100000000420069020000000400000000000042000D020000000400000001000000004200F010000005842005A050000000400000011000000004200760100000040420091070000002434666563336135392D623231372D346162662D383461642D616631353437303234363135000000004200930400000008000000000000001F4</p> <p>Out: uuidKey</p> <p>Tag: Response Message (0x420078), Type: Structure (0x01), Data:</p> <p>Tag: Response Header (0x420077), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420067), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Time Stamp (0x42008F), Type: Date-Time (0x09), Data: 0x000000004AC0782B (Mon Sep 28 10:47:39 CEST 2009)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x4200F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)</p> <p>Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000001 (Failed)</p> <p>Tag: Result Reason (0x42007B), Type: Enumeration (0x05), Data: 0x0000000C (Permission Denied)</p> <p>Tag: Result Message (0x42007A), Type: Text String (0x07), Data: Unable to allocate requested byte amount</p> <p>42007801000000B84200770100000048420067010000002042006802000000040000000100000000420069020000000400000000000042008F0900000008000000004AC0782B42000D020000000400000001000000004200F010000006042005A0500000004000000110000000042007C0500000004000000010000000042007B05000000040000000C0000000042007A0700000028556E61626C6520746F20616C6C6F6361746520726571756573746564206279746520616D6F756E74</p>
10	<p>Client A:</p> <p>Destroy (symmetric key)</p> <p>In: uuidKey</p> <p>Tag: Request Message (0x420075), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (0x420074), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420067), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x4200F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</p> <p>Tag: Request Payload (0x420076), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615</p> <p>42007501000000904200740100000038420067010000002042006802000000040000000100000000420069020000000400000000000042000D020000000400000001000000004200F010000004842005A050000000400000014000000004200760100000040420091070000002434666563336135392D623231372D346162662D383461642D616631353437303234363135000000004200930400000008000000000000001F4</p>

760100000030420091070000002434666563336135392D623231372D346162662D383461642D61663135343730323436313500000000

Out: uuidKey

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: 0x000000004AC0782C (Mon Sep 28 10:47:40 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: 0x00000014 (Destroy)
Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 4fec3a59-b217-4abf-84ad-af1547024615

42007801000000B04200770100000048420067010000002042006802000000040000000100000000420069020000000400000000000042008F0900000008000000004AC0782C42000D0200000004000000010000000042000F010000005842005A0500000004000000140000000042007C05000000040000000000000004200790100000030420091070000002434666563336135392D623231372D346162662D383461642D61663135343730323436313500000000

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	<p>Register (symmetric key) In: objectType = '00000002', attributes={ CryptographicUsageMask='00000004' }, foreignSymmetricKey</p> <p>Tag: Request Message (0x420075), Type: Structure (0x01), Data: Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p>

Mask

Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000003 (Register)

Tag: Request Payload (0x420076), Type: Structure (0x01), Data:

Tag: Object Type (0x420055), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Template-Attribute (0x42008E), Type: Structure (0x01), Data:

Tag: Attribute (0x420008), Type: Structure (0x01), Data:

Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage

Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt)

Tag: Symmetric Key (0x42008C), Type: Structure (0x01), Data:

Tag: Key Block (0x42003E), Type: Structure (0x01), Data:

Tag: Key Format Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001

Tag: Key Value (0x420043), Type: Structure (0x01), Data:

Tag: Key Material (0x420041), Type: Octet String (0x08), Data: 0123456789ABCDEF0123456789ABCDEF

Tag: Cryptographic Algorithm (0x420026), Type: Enumeration (0x05), Data: 0x00000003 (AES)

Tag: Cryptographic Length (0x420028), Type: Integer (0x02), Data: 0x00000080 (128)

4200750100000110420074010000003842006701000000204200680200000004000000010000000042006902000000040
0000000000000042000D0200000004000000010000000042000F01000000C842005A0500000004000000030000000042
007601000000B04200550500000004000000020000000042008E0100000038420008010000003042000A0700000018437
27970746F67726170686963205573616765204D61736B42000B0200000004000000040000000042008C01000000584200
3E010000005042004005000000040000000100000000420043010000001842004108000000100123456789ABCDEF01234
56789ABCDEF42002605000000040000000300000000420028020000000400000008000000000

Out: uuidKey

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: 0x000000004AC0782C (Mon Sep 28 10:47:40 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: 0x00000003 (Register)

Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: bb806453-5c75-42c2-80bd-4e52f1ceb57b

42007801000000B0420077010000004842006701000000204200680200000004000000010000000042006902000000040
0000000000000042008F0900000008000000004AC0782C42000D0200000004000000010000000042000F010000005842
005A0500000004000000030000000042007C0500000004000000000000000042007901000000304200910700000024626
23830363435332D356337352D343263322D383062642D34653532663163656235376200000000

1	<p>Add attribute</p> <p>In: uuidKey, attribute={ x-provider='unknown' }</p> <p>Tag: Request Message (0x420075), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (0x420074), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420067), Type: Structure (0x01), Data:</p>
---	--

Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x420069), 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 (0x42005A), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: bb806453-5c75-42c2-80bd-4e52f1ceb57b
 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

42007501000000C0420074010000003842006701000000204200680200000004000000010000000042006902000000040
 0000000000000042000D0200000004000000010000000042000F010000007842005A05000000040000000D0000000042
 00760100000060420091070000002462623830363435332D356337352D343263322D383062642D3465353266316365623
 5376200000000420008010000002842000A070000000A782D70726F76696465720000000000042000B0700000007756E
 6B6E6F776E00

Out: uuidKey, attribute={ x-provider='unknown' }

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: 0x000000004AC0782E (Mon Sep 28 10:47:42 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: 0x0000000D (Add Attribute)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: bb806453-5c75-42c2-80bd-4e52f1ceb57b
 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

42007801000000E0420077010000004842006701000000204200680200000004000000010000000042006902000000040
 0000000000000042008F0900000008000000004AC0782E42000D0200000004000000010000000042000F010000008842
 005A05000000040000000D0000000042007C050000000400000000000000042007901000000604200910700000024626
 23830363435332D356337352D343263322D383062642D3465353266316365623537620000000042000801000000284200
 0A070000000A782D70726F76696465720000000000042000B0700000007756E6B6E6F776E00

2

Modify attribute
In: uuidKey, attribute={ x-provider='third party' }

Tag: Request Message (0x420075), Type: Structure (0x01), Data:
 Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
 Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: bb806453-5c75-42c2-80bd-4e52f1ceb57b
 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

42007501000000C8420074010000003842006701000000204200680200000004000000010000000042006902000000040
 00000000000000042000D0200000004000000010000000042000F010000008042005A05000000040000000E0000000042
 00760100000068420091070000002462623830363435332D356337352D343263322D383062642D3465353266316365623
 5376200000000420008010000003042000A070000000A782D70726F76696465720000000000042000B070000000B7468
 6972642070617274790000000000

Out: uuidKey, attribute={ x-provider='third party' }

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: 0x000000004AC0782E (Mon Sep 28 10:47:42 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: 0x0000000E (Modify Attribute)
 Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: bb806453-5c75-42c2-80bd-4e52f1ceb57b
 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

42007801000000E8420077010000004842006701000000204200680200000004000000010000000042006902000000040
 00000000000000042008F0900000008000000004AC0782E42000D0200000004000000010000000042000F010000009042
 005A05000000040000000E0000000042007C050000000400000000000000042007901000000684200910700000024626
 23830363435332D356337352D343263322D383062642D3465353266316365623537620000000042000801000000304200
 0A070000000A782D70726F76696465720000000000042000B070000000B74686972642070617274790000000000

3	<p>Destroy (symmetric key)</p> <p>In: uuidKey</p> <p>Tag: Request Message (0x420075), Type: Structure (0x01), Data: Tag: Request Header (0x420074), 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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p>
---	--

```

Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
Tag: Request Payload (0x420076), Type: Structure (0x01), Data:
  Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: bb806453-5c75-42c2-80bd-4e52f1ceb57b

4200750100000090420074010000003842006701000000204200680200000004000000010000000042006902000000040
000000000000042000D0200000004000000010000000042000F010000004842005A0500000004000000140000000042
00760100000030420091070000002462623830363435332D356337352D343263322D383062642D3465353266316365623
5376200000000

Out: uuidKey

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: 0x000000004AC0782E (Mon Sep 28
10:47:42 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: 0x00000014 (Destroy)
    Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: bb806453-5c75-42c2-80bd-4e52f1ceb57b

42007801000000B0420077010000004842006701000000204200680200000004000000010000000042006902000000040
0000000000000042008F0900000008000000004AC0782E42000D0200000004000000010000000042000F010000005842
005A0500000004000000140000000042007C0500000004000000000000000042007901000000304200910700000024626
23830363435332D356337352D343263322D383062642D34653532663163656235376200000000

```

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', CryptographicUsageMask='0000000C' }, MessageExtension={ VendorIdentification='Acme',

	<p>CriticalityIndicator='false', VendorExtension={ tag='0x540001', type='text string', value='na' } }</p> <p>Out: objectType='00000002', uuidKey</p>
1	<p>Destroy (symmetric key)</p> <p>In: uuidKey</p> <p>Out: uuidKey</p>

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	<p>Create (symmetric key)</p> <p>In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C' }, MessageExtension={ VendorIdentification='Acme', CriticalityIndicator='true', VendorExtension={ tag='0x540001', type='text string', value='na' } }</p> <p>Out: Operation Failed, Feature Not Supported</p>

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	<p>Create Key Pair</p> <p>In: commonAttributes={ CryptographicAlgorithm='RSA', CryptographicLength='1024', CryptographicUsageMask='0000000C' }, privateKeyAttributes={ Name={ NameValue='PrivateKey1', NameType='00000001' } }, publicKeyAttributes={ NameValue='PublicKey1', NameType='00000001' } }</p>

	Out: uuidPrivateKey, uuidPublicKey
1	Locate (Public Key) In: attributes={ objectType='PublicKey', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } } Out: uuidPublicKey
2	Locate (Private Key) In: attributes={ objectType='PrivateKey', Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } } Out: uuidPrivateKey
3	Destroy In: uuidPrivateKey Out: uuidPrivateKey
4	Destroy In: uuidPublicKey Out: uuidPublicKey

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

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

Time	Client A
0	Register (Private Key) In: objectType='00000004', attributes={ CryptographicUsageMask='0000000C' }, foreignPrivateKey Out: uuidPrivateKey
1	Register (Public Key) In: objectType='00000004', attributes={ CryptographicUsageMask='0000000C', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } }, foreignPublicKey Out: uuidPublicKey
2	Add attribute In: uuidPrivateKey, attribute={ Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } } Out: uuidPrivateKey, attribute={ Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } }
3	Locate (Public Key) In: attributes={ objectType='PublicKey', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } } Out: uuidPublicKey
4	Locate (Private Key) In: attributes={ objectType='PrivateKey', Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } }

	Out: uuidPrivateKey
5	Destroy In: uuidPrivateKey Out: uuidPrivateKey
6	Destroy In: uuidPublicKey Out: uuidPublicKey

9 Key Roll-over

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

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

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

Time	Client A
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='rekeyKey', NameType='00000001' } } Out: objectType='00000002', uuidKey
1	Locate In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Out: uuidKey
2	Rekey In: uuidKey Out: uuidNewKey
3	Locate In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Out: uuidNewKey
4	Get Attribute In: uuidKey, attributeName={'Name'} Out: Operation Failed, Item Not Found
5	Get (symmetric key)

	In: uuidKey Out: objectType = '00000002', uuidKey, symmetricKey
6	Destroy In: uuidKey Out: uuidKey
7	Destroy In: uuidNewKey Out: uuidNewKey

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

Create a new symmetric key with a name. Then add the *Activation Date* and *Deactivation Date* attributes based on the timestamp in the response to the Create request. The *Activation Date* is set to a time in the past and the *Deactivation Date* to a time in the near future. Repeated Get Attribute calls are performed to verify that the state is first "Active", then subsequently "Deactive". Then issue a Re-key request, including an *Activation Date* attribute with the value set to the previously specified *Deactivation Date* of the existing key. Verify from the response that the *Activation Date* and *Deactivation Date* attributes were set correctly (if they are not returned, issue a Get Attribute request). 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', CryptographicUsageMask='0000000C' } Out: objectType='00000002', uuidKey
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>' } Out: uuidKey, attribute={ ActivationDate=' <Timestamp in previous response - 1 year>' } Out: uuidKey, attribute={ DeactivationDate=' <Timestamp in previous response + 2 minutes>' }
2	Get Attribute * Repeated until state changes to Deactivated In: uuidKey, attributeName={'State'} Out: uuidKey, attribute={ State='Active' }
3	Get Attribute In: uuidKey, attributeName={'State'} Out: uuidKey, attribute={ State='Deactive' }
4	Rekey In: uuidKey, attribute={ offset='018B8200' (300 days)} Out: uuidNewKey

5	<p>Get Attribute</p> <p>In: uuidNewKey, attributeName={ ' ActivationDate', ' DeactivationDate' }</p> <p>Out: uuidNewKey, attribute={ ActivationDate=' <Value of ActivationTime in existing key + 300 days>', DeactivationDate='<Value of DeactivationDate of existing key + 300 days>' }</p>
6	<p>Get Attribute</p> <p>In: uuidNewKey, attributeName={ 'State' }</p> <p>Out: uuidNewKey, attribute={ State='Active' }</p>
7	<p>Destroy</p> <p>In: uuidKey</p> <p>Out: uuidKey</p>
8	<p>Destroy</p> <p>In: uuidNewKey</p> <p>Out: uuidNewKey</p>

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	<p>Create (symmetric key)</p> <p>In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='rekeyKey', NameType='00000001' }, ActivationDate='2' }</p> <p>Out: objectType='00000002', uuidKey</p>
1	<p>Get Attribute</p> <p>In: uuidKey, attributeName={ 'State' }</p> <p>Out: uuidKey, attribute={ State='Active' }</p>
2	<p>Revoke (symmetric key as compromised)</p> <p>In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceDate='6'</p> <p>Out: uuidKey</p>
3	<p>Get Attribute</p> <p>In: uuidKey, attributeName={ 'State' }</p> <p>Out: uuidKey, attribute={ State='Compromised' }</p>
4	<p>Rekey</p> <p>In: uuidKey, offset='0'</p> <p>Out: uuidNewKey</p>

5	Get Attribute In: uuidNewKey, attributeName={ 'State' } Out: uuidNewKey, attribute={ State='Active' }
6	Destroy In: uuidKey Out: uuidKey
7	Destroy In: uuidNewKey Out: uuidNewKey

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

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

Time	Client A
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='rekeyKey', NameType='00000001' } } Out: objectType='00000002', uuidKey
1	Locate In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Out: uuidKey
2	Rekey In: uuidKey, attributes={ ActivationDate='0000000043B7B630', ProcessStartDate='0000000043B7B630', ProtectStopDate='000000005E0C7BB0', DeactivationDate='000000005E0C7BB0' } Out: uuidNewKey
3	Get Attribute In: uuidKey, attributeName={ 'Name' } Out: Operation Failed, Item Not Found
4	Get Attribute In: uuidKey, attributeName={ 'ActivationDate', 'ProcessStartDate', 'ProtectStopDate', 'DeactivationDate' } Out: uuidKey, attribute={ ActivationDate='0000000043B7B630', ProcessStartDate='0000000043B7B630', ProtectStopDate='000000005E0C7BB0', DeactivationDate='000000005E0C7BB0' }
5	Locate In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Out: uuidNewKey

6	Destroy In: uuidKey Out: uuidKey
7	Destroy In: uuidNewKey Out: uuidNewKey

9.5 Use-case: Obtain Lease for Expired Key

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

Time	Client A	Client B
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue=' rekeyKey', NameType='00000001' }, ActivationDate='2' } Out: objectType='00000002', uuidKey	
1	Get (symmetric key) In: uuidKey Out: objectType = '00000002', uuidKey, symmetricKey	
2	Obtain Lease In: uuidKey Out: uuidKey, leaseTime, lastChangeDate	
3		Revoke (symmetric key as compromised) In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceDate='6' Out: uuidKey
4		Rekey In: uuidKey, offset='0' Out: uuidNewKey
5	Obtain Lease In: uuidKey Out: Operation Failed, Permission Denied	

6	Locate (symmetric key) In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Out: uuidNewKey	
7	Get (symmetric key) In: uuidNewKey Out: objectType = '00000002', uuidNewKey, newSymmetricKey	
8	Obtain Lease In: uuidNewKey Out: uuidNewKey, leaseTime, lastChangeDate	
9	Destroy In: uuidKey Out: uuidKey	
10	Destroy In: uuidNewKey Out: uuidNewKey	

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

Time	Client A
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='archiveKey', NameType='00000001' } } Out: objectType='00000002', uuidKey
1	Locate In: attributes={ Name={ NameValue='archiveKey', NameType='00000001' } } Out: uuidKey
2	Get (symmetric key)

	In: uuidKey Out: objectType = '00000002', uuidKey, symmetricKey
3	Archive In: uuidKey, asynchronousIndicator='true' Out: asynchronousCorrelationValue
4	Poll* In: asynchronousCorrelationValue Out: uuidKey
5	Get (symmetric key) In: uuidKey Out: Operation Failed, Item Not Found
6	Locate In: attributes={ Name={ NameValue='archiveKey', NameType='00000001' } } Out: Operation Failed, Item Not Found
7	Locate In: storageStatusMask='00000003', attributes={ Name={ NameValue='archiveKey', NameType='00000001' } } Out: uuidKey
8	Recover In: uuidKey, asynchronousIndicator='true' Out: asynchronousCorrelationValue
9	Poll* In: asynchronousCorrelationValue Out: uuidKey
10	Get (symmetric key) In: uuidKey Out: objectType = '00000002', uuidKey, symmetricKey
11	Destroy In: uuidKey Out: uuidKey

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:

Gordon Arnold, IBM
Todd Arnold, IBM
Matthew Ball, Sun Microsystems
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, HP
Indra Fitzgerald, HP
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.
Marc Hocking, BeCrypt Ltd.
Larry Hofer, Emulex Corporation
Brandon Hoff, Emulex Corporation
Walt Hubis, LSI Corporation
Wyllys Ingersoll, Sun Microsystems
Jay Jacobs, Target Corporation
Glen Jaquette, IBM

Scott Kipp, Brocade Communications Systems, Inc.
David Lawson, Emulex Corporation
Robert Lockhart, Thales e-Security
Shyam Mankala, EMC Corporation
Marc Massar, Individual
Don McAlister, Cipheroptics
Hyrum Mills, Mitre Corporation
Landon Noll, Cisco Systems, Inc.
René Pawlitzek, IBM
Rob Philpott, EMC Corporation
Bruce Rich, IBM
Scott Rotondo, Sun Microsystems
Anil Saldhana, Red Hat
Subhash Sankuratipati, NetApp
Mark Schiller, HP
Jitendra Singh, Brocade Communications Systems, Inc.
Servesch Singh, EMC Corporation
Sandy Stewart, Sun Microsystems
Marcus Streets, Thales e-Security
Brett Thompson, SafeNet, Inc.
Benjamin Tomhave, Individual
Sean Turner, IECA, Inc.
Paul Turner, Venafi, Inc.
Marko Vukolic, IBM
Rod Wideman, Quantum Corporation
Steven Wierenga, HP
Peter Yee, EMC Corporation
Krishna Yellepeddy, IBM
Peter Zelechowski, Election Systems & Software

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.