TBD (Key Management Interoperability Protocol Use Cases)

Committee Draft 1.0

8 October 2009

Specification URIs:
This Version:
TBD.html
TBD.doc (Authoritative)
TBD.pdf
Previous Version:
TBD.html
TBD.doc (Authoritative)
TBD.pdf
Latest Version:
TBD.html
TBD.doc
TBD.pdf
Technical Committee:
OASIS Key Management Interoperability Protocol (KMIP) TC
Chair(s):
Robert Griffin
Anthony Nadalin
Editor(s):
Mathias Björkqvist
René Pawlitzek
Related work:
This specification replaces or supersedes:

- None

This specification is related to:

- TBD

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

Deleted: Editor's
Deleted: 0.98
Deleted: 28 September
Deleted: Declared XML Namespace(s):¶ TBD¶
Deleted: -0.98
Deleted: 28 September

"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/.

Deleted: -0.98

Deleted: 28 September

Notices

Deleted: -0.98

Deleted: 28 September

Table of Contents

Deleted: 1 Introduction . 5¶
1.1 Document Roadmap . 5¶
1.2 Goals and Requirements . 5¶
1.3 Notational Conventions . 5¶
1.4 Namespaces . 5¶
1.5 Terminology . 5¶
1.6 Normative References . 5¶
1.7 Non-normative References . 5¶
1.8 Compliance . 5¶
2 Message exchange . 6¶
3 Centralized Management . 6¶
3.1 Basic functionality . 6¶
3.1.1 Use-case: Create / Destroy . 6¶
3.1.2 Use-case: Register / Create / Get attributes / Destroy . 8¶
3.1.3 Use-case: Create / Locate / Get / Destroy . 14¶
3.1.4 Use-case: Dual client use-case, ID Placeholder linked Locate & Get batch . 19¶
3.2 Use-case: Asynchronous Locate . 34¶
4 Key life cycle support . 44¶
4.1 Use-case: Revoke scenario . 44¶
5 Auditing and reporting . 61¶
5.1 Use-case: Get usage allocation scenario . 61¶
6 Key Interchange, Key Exchange . 72¶
6.1 Use-case: Import of a Third-party Key . 73¶
7 Vendor Extensions . 77¶
7.1 Use-case: Unrecognized Message Extension with Criticality Indicator false . 77¶
7.2 Use-case: Unrecognized Message Extension with Criticality Indicator true . 77¶
8 Asymmetric keys . 78¶
8.1 Use-case: Create a Key Pair . 78¶
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 . 85¶
A. . Acknowledgments . 87¶
B. . Revision History . 88¶

Deleted: -0.98

Deleted: 28 September

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 v0.98 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] draft, ***KMIP Specification***, Approval Date, URI (TBD)

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='00000002' (Symmetric Key), attributes={ CryptographicAlgorithm='00000003' (AES), CryptographicLength='128', CryptographicUsageMask='0000000C' }

Formatted: Font: Bold
Deleted: shall
Formatted: Font: Bold
Deleted: can be used to
Deleted: may or may not be omitted
Deleted: will
Formatted: Bullets and Numbering
Deleted: ¶
<#>Document Roadmap¶
TBD¶
<#>Goals and Requirements¶
TBD¶
<#>Notational Conventions¶
TBD¶
<#>Namespaces¶
TBD¶
<#>Terminology¶
TBD¶
<#>Normative References¶
TBD¶
<#>Non-normative References¶
TBD¶
<#>Compliance¶
TBD¶
Deleted: shall happen
Deleted: -0.98
Deleted: 28 September

```
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)


42007501000001204200740100000038420067010000002042006802000000040000000000000000420069020000000400000062000000004200D020000000400000001000000004200F01000000D842005A050000000400000010000000042007601000000C042005505000000040000000200000000042008E01000000A84200080100000030420000A0700000017437279707466772617068696320416C676F726974686D0042000B050000000400000003000000004200080100000030420000A070000001443727970746F67726170686963204C656E677468000000004200B020000000400000080000000004200801000000030420000A070000001843727970746F6772617068696320557361676520 4D61736B42000B0200000004000000C00000000


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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
      Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 46eca90a-4b20-423c-
b968-750f299f0ca7


42007801000000C042007701000000484200670100000020420068020000000400000000000000004200690200000004
00000062000000004200 8F090000000800000000 4AC0731C42000D020000000400000001000000004200F0100000068
```

Deleted: -0.98

Deleted: 28 September

	42005A0500000004000000010000000042007C0500000004000000000000000042007901000000404200550500000004000000020000000042009107000000243436656361393061 2D346232302D343233632D623936382D3735306632393966 3063613700000000
1	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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400000062000000004200 0D020000000400000001000000042000F0100000048420 05A0500000004000000140000000042007601000000304200910700000024343665636139306 12D346232302D343233632D623936382D3735306632393966 3063613700000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000004200 8F090000000800000000 4AC0731D42000D020000000400000001000000004200 0F0100000058420 05A0500000004000000140000000042007C0500000004000000000000000042007901000000304200910700000024343665636139306 12D346232302D343233632D623936382D3735306632393966306361370000000

Deleted: -0.98

Deleted: 28 September

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	Register (template) In: objectType='00000007', attributes={ ObjectGroup='Group1', ApplicationSpecificInformation='ssl, www.example.com', ContactInformation='Joe', x-Purpose='demonstration', Name={ NameValue='Template1', 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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: Object Group Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Application Specific Information Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Application Namespace (0x420003), Type: Text String (0x07), Data: ssl Tag: Application Data (0x420002), Type: Text String (0x07), Data: www.example.com Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-Purpose Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: demonstration Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420053), Type: Text String (0x07), Data: Template1 Tag: Name Type (0x420052), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007501000001C042007401000000384200670100000020420068020000000400000000000000004200690200000004000000062000000004200 0D020000000400000001000000042000F01000001784200 5A05000000040000000300000000420076010000016042005505000000040000000600000000420 08E01000001484200080100000028420 00A070000000C4F626A6563742047726F7570000000004200 0B070000000647726F75703100004200080100000058420 00A07000000204170706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000B01000000284200030700000373736C0000000004200207000000 0F7777772E6578616D706C652E636F6D0042000801000000 3042000A0700000013436F6E	**Deleted:** -0.98 **Deleted:** 28 September

7461637420496E666F726D6174696F6E00000000042000B070000000034A6F650000000004200080100000030420000A0700000009782D507572706F7365000000000000000042000B070000000D64656D6F6E7374726174696F6E00000042000801000000404200 0A07000000044E616D650000000042000B0100000028420053070000000954656D706C617465310000000000000042005205000000040000000100000000

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000004200 8F090000000800000000 4AC0731E42000D020000000400000001000000004200 0F010000005842005A0500000004000000030000000042007C0500000004000000000000000042007901000000304200910700000024346663336634373 32D346465342D343234382D393930652D323165303066376663303036000000000

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
```

Deleted: -0.98

Deleted: 28 September

	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) 42007501000001504200740100000038420067010000002042006802000000040000000000000000420069020000000400000006200000000042000D020000000400000001000000004200 0F0100000108420005A0500000004000000010000000042007601000000F042005505000000040000000200000000042008E01000000D84200510100000028420053070000000954656D706C6174653100000000000000042005205000000040000000100000000420008010000003042000A07000000174372797074 6F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200 0A0700000014437279707 46F6772617068696320 4C656E67746800000000042000B020000000400000008000000000420008 0100000030420 00A0700000018437279707 46F6772617068696320557361676520 4D61736B42000B020000000400000000 C00000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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-7ce119896608 42007801000000C042007701000000484200670100000020420068020000000400000000000000004200690200000004 0000006200000000042008F090000000800000004AC0731F42000D020000000400000001000000004200 0F010000006842 005A0500000004000000010000000042007C0500000004000000000000000042007901000000404200550500000004000 0000200000000042009107000000243330303838316338 2D353936612D343861642D383134662D376365313139383936363 03800000000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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-7ce119896608

Deleted: -0.98

Deleted: 28 September

```
      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
```

```
42007501000001084200740100000038420067010000002042006802000000040000000000000000420069020000000400
000006200000000042000D020000000400000001000000042000F01000000C042005A0500000004000000B0000000042
007601000000A842009107000000243330303838316338 2D353936612D343861642D383134662D376365313139383936 3
6303800000000042000A070000000C4F626A6563742047726F757000000000042000A0700000020417070 6C69636174696F
6E20537065636966696320496E666F726D6174696F6E42000A0700000013436F6E746163742049 6E666F726D6174696F6
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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-
7ce119896608
      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
```

```
42007801000001B042007701000000484200670100000020420068020000000400000000000000004200690200000004 0
0000062000000004200 8F090000000800000000 4AC0731F42000D020000000400000001000000004200 0F010000015842
005A0500000004000000 0B000000004200 7C050000000400000000000000004200 790100000013042009107000000024333
03038383163382D353936612D343861642D383134662D376365313139383936363038000000042000801000000284200
0A070000000C4F626A6563742047726F757000000000042000B070000000647726F757031000042000801000000584200 0
A0700000020417070 6C69636174696F6E20537065636966696320496E666F726D6174696F6E42000B0100000028420003
0700000003737360000000000042000207000000F777772E6578616D706C652E636F6D0042000801000000300420 00A0
700000013436F6E746163742049 6E666F726D6174696F6E000000000042000B07000000034A6F650000000000420008 01
```

Deleted: -0.98

Deleted: 28 September

	0000003042000A0700000009782D507572706F7365000000000000042000B070000000D64656D6F6E7374726174696F6E000000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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-7ce119896608 42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400000006200000000042000D020000000400000001000000042000F010000004842005A050000000400000014000000004200790100000030420091070000002433303038383163382D353936612D343861642D383134662D376365313139383936303800000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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-7ce119896608 42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000004200F090000000800000004AC0732042000D020000000400000001000000042000F010000005842005A050000000400000014000000004200C050000000400000000000000004200790100000030420091070000002433303038383163382D353936612D343861642D383134662D376365313139383936303800000000
4	Destroy (template) In: uuidTemplate 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: 0x00000000 (0)

Deleted: -0.98

Deleted: 28 September

	Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400000006200000000420 00D020000000400000001000000004200 0F010000004842005A0500000004000000140000000042007601000000304200910700000024346663336634373 32D346465342D343234382D393930652D3231653030663766633 0303600000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004 0000062000000000420 08F0900000008000000004AC0732042000D020000000400000001000000004200 0F010000005842 005A0500000004000000140000000042007C0500000004000000000000000042007901000000304200910700000024346 66333663437332D346465342D343234382D393930652D3231653030663766633030360000000

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' }

Deleted: -0.98

Deleted: 28 September

```
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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


42007501000001984200740100000038420067010000002042006802000000040000000000000004200690200000004
0000006200000000042000D020000000400000001000000042000F01000001504200 5A0500000004000000010000000042
00760100000138420055050000000400000002000000042008E01000001204200080100000038420 00A07000000044E6
16D650000000042000B01000000204200530700000044B6579310000000042005205000000040000001000000004200
0801000000304200 0A0700000017437279707 46F6772617068696320416C676F726974686D0042000B050000000400000
0010000000042000801000000304200 0A0700000014437279707 46F67726170686963204C656E6774680000000042000B
020000000400000038000000004200080100000030420 00A0700000018437279707 46F67726170686963205573616765 2
04D61736B42000B020000000400000000C000000004200080100000030420 00A0700000013436F6E746163742049 6E666F
726D6174696F6E000000000042000B07000000034A6F650000000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
```

Deleted: -0.98

Deleted: 28 September

```
  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: 75da9bc9-7867-49c5-886d-
757f3d523d3f


42007801000000C042007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000004200
8F090000000800000004AC0732142000D020000000400000001000000004200
0F010000006842005A05000000040000000100000000420070500000000400000001000000042007901000000404200550500000004000000020
000000004200910700000024373564613962633920373836372D343963352D383836642D373537663364354323633643366000000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)


42007501000000D042007401000000384200670100000020420068020000000400000000000000004200690200000004000000062000000004200
0D020000000400000001000000004200
0F010000008842005A05000000040000000800000000420076010000007042000801000000284200
0A070000000B4F626A6563742054797065000000000042000B0500000004000000020000000042000801000000384200
0A07000000044E616D650000000042000B010000002042005307000000044B657931000000004200520500000004000000010000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008F), Type: Date-Time (0x09), Data: 0x000000004AC07321 (Mon Sep 28
10:26:09 CEST 2009)
```

Deleted: -0.98

Deleted: 28 September

```
    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
```

```
42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000
0000062000000004200 8F090000008000000004AC0732142000D020000000400000001000000004200 0F010000005842
005A0500000004000000080000000042007C0500000004000000000000000042007901000000304200910700000024373
56461396263392D373836372D343963352D383836642D373537663364353233643360000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400
0000062000000004200 0D020000004000000010000000042000 F010000004842005A0500000004000000 0A0000000042
00760100000030420091070000002437356461396263392D373836372D343963352D383836642D3735376633643532336
4336600000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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:
```

Deleted: -0.98

Deleted: 28 September

```
          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)
```

```
42007801000001184200770100000048420067010000002042006802000000040000000000000000420069020000000400
00000620000000042008F090000000800000004AC0732242000D020000000400000001000000004200 0F01000000C042
005A0500000004000000 0A0000000042007C0500000004000000000000000042007901000000984200550500000004000
0000200000000420091070000002437356461396263392D373836372D343963352D383836642D3735376633643532336 4
33660000000042008C010000005042003E0100000048420040050000000400000001000000004200430100000010420041
10800000008EAD09734B085DFFE42002605000000040000000100000000420028020000000400000038000000 00
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400
00000620000000042000D020000000400000001000000004200 0F0100000048420 05A0500000004000000140000000042
00760100000030420091070000002437356461396263392D373836372D343963352D383836642D3735376633643532336
4336600000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
42007801000000B04200770100000048420067010000002042006802000000040000000000000000420069020000000400
00000620000000042008F090000000800000004AC0732242000D020000000400000001000000004200 0F010000005842
```

Deleted: -0.98

Deleted: 28 September

	005A0500000004000000140000000042007C0500000004000000000000000042007901000000304200910700000024373564613962633 92D373836372D343963352D383836642D373537663364353233643366000000000
4	Locate 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000B84200740100000038420067010000002042006802000000040000000000000000420069020000000400000062000000004200 0D020000000400000001000000004200 0F01000000704200 5A05000000040000000800000000420 07C0500000004000000000000000042007901000000004200760100000058420008010000005042000A0700000011556E6971756520496465 6E7469666965720000000000000042000B070000000243735646139626339 2D373836372D343963352D383836642D373537663364353233643366000000000 Out: <empty response payload> Tag: Response Message (0x420078), Type: Structure (0x01), Data: Tag: Response Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420067), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007801000000804200770100000048420067010000002042006802000000040000000000000000420069020000000400000062000000004200 8F090000000800000000 4AC0732342000D020000000400000001000000004200 0F010000002842005A05000000040000000800000000420 07C0500000004000000000000000042007901000000000

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

Deleted: -0.98

Deleted: 28 September

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.

Deleted: may

Deleted: would

Time	Request/Response messages
0	Client A: Register (template) In: objectType='00000007', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', Name={ NameValue='Template1', 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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) 42007501000001304200740100000038420067010000002042006802000000040000000000000000420069020000000400000062000000004200 0D020000000400000001000000004200 0F01000000E842005A0500000004000000030000000042007601000000D042005505000000040000000600000000042008E01000000B842000801000000304200A0700000014437279707 46F67726170686963204 16C676F726974686D0042000B0500000004000000030000000042000801000000304200A0700000014437279707 46F67726170686963204 C656E6774680000000042000B020000000400000080000000004200080100000040420 00A07000000044E616D650000000042000B0100000028420053070000000954656D706C617465310000000000000042005205000000040000000100000000 Out: uuidTemplate

Deleted: -0.98

Deleted: 28 September

```
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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


42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000004200
8F090000000800000004AC0732342000D020000000400000001000000004200
0F010000005842005A0500000004000000030000000042007C050000000400000000000000004200790100000030420091070000002438333833313938622D343630302D343338382D393535662D323830326363363939653963000000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
```

Deleted: -0.98

Deleted: 28 September

	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 42007501000001584200740100000038420067010000002042006802000000040000000000000000420069020000000400000062000000042000D020000000400000001000000042000F0100000011042005A0500000004000000010000000420076010000F84200550500000004000000020000000042008E01000000E042005101000000284200530700000009546 56D706C6174653100000000000000042005205000000040000001000000004200080100000038420 00A07000000044E616D6500000000042000B0100000020420053070000000 44B6579310000000042005205000000040000000100000000420008010000003042000A0700000018437279707 46F6772617068696320557361676520 4D61736B42000B0200000004000000040000000042000801000000304200 0A0700000013436F6E7461637420496E666F726D6174696F6E00000000042000B0700000003466F6F0000000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007801000000C042007701000000484200670100000020420068020000000400000000000000004200690200000004000000620000000042008F090000000800000004AC0732442000D020000000400000001000000004200 0F010000006842005A0500000004000000010000000042007C0500000004000000000000000042007901000000404200550500000004000000020009107000000243766626130383439 2D613363322D346438632D383164642D396131393939343765343764000000000 Out: <empty Get payload>
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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)

Deleted: -0.98

Deleted: 28 September

```
    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


42007501000001204200740100000048420067010000002042006802000000040000000000000000420069020000000400
00000620000000042001006000000080000000000000000142000D020000000400000002000000004200 0F010000009842
005A0500000004000000080000000042009008000000801F76942FF5A7A8A42007601000000704200080100000028420
00A070000000B4F626A6563742054797065000000000042000B0500000004000000020000000042000801000000384200
0A07000000044E616D650000000042000B0100000020420053070000000 44B6579310000000042005205000000040000000
0010000000042000F01000002842005A0500000004000000 0A000000004200900800000083192EDD439D59CC4420076
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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:
```

Deleted: -0.98

Deleted: 28 September

```
        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)
```

```
42007801000001A042007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000042008F090000000800000004AC0732442000D020000000400000002000000004200F010000006842005A0500000004000000080000000042009008000000801F76942FF5A7A8A42007C0500000004000000000000000042007901000000304200910700000024376662613038343920D613363322D346438632D383164642D3961313939393437653437640000000042000F01000000D842005A0500000004000000A0000000042009008000000083192EDD439D59CC442007C0500000004000000000000000042007901000000A042005505000000040000000200000000420091070000002437666261303834392D613363322D346438632D383164642D3961313939393437653437640000000042008C010000005842003E0100000504200400500000004000000010000000042004301000000184200410800000105C7B76DC93EF45FD9231522EB2CE7B0A42002605000000040000000300000000420028020000000400000080000000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400000006200000000042000D020000000400000001000000004200F01000000484200 5A0500000004000000C0000000042007601000000304200910700000024376662613038343920D613363322D346438632D383164642D39613139393934376534376400000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
```

Deleted: -0.98

Deleted: 28 September

	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 42007801000001D042007701000000484200670100000020420068020000000400000000000000004200690200000004000000620000000042008F090000000800000004AC0732542000D020000000400000001000000042000F010000017842005A0500000004000000C0000000042007C0500000004000000000000000042007901000001504200910700000024376662613038343926133633223436438632D383164642D396131393939343765343764000000042000A07000000144372797074 6F6772617068696320 4C656E6774680000000042000A0700000017437279707 46F6772617068696320416C676F726974686D0042000A0700000005537461746500000042000A0700000006446967657374000042000A070000000C496E697469616C20446174650000000042000A0700000011556E6971756204964656E74696669657200000000000000042000A07000000044E616D650000000042000A0700000018437279707 46F6772617068696320 55736161765204D61736B42000A070000000B4F626A65637420547970650000000000042000A0700000013436F6E7461637420496E666F726D6174696F6E000000000042000A07000000114C617374204368616E676564204461746500000000000000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000C042007401000000384200670100000020420068020000000400000000000000004200690200000004000000620000000042000D020000000400000001000000042000F010000007842005A0500000004000000B0000000420076010000006042009107000000243766626130383439 2D613363322D346438632D383164642D396131393939343765343764000000042000A07000000044E616D650000000042000A0700000013436F6E7461637420496E666F726D6174696F6E0000000000 Out: uuidKey, attributes={ Name={ Name='Key1', NameType='00000001' }, ContactInformation='Foo' } Tag: Response Message (0x420078), Type: Structure (0x01), Data:

Deleted: -0.98

Deleted: 28 September

```
  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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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


42007801000001284200770100000048420067010000002042006802000000040000000000000000420069020000000400
00000620000000042008F090000000800000004AC0732542000D020000000400000001000000004200 0F01000000D042
005A0500000004000000B0000000042007C0500000004000000000000000042007901000000A842009107000000024376
66261303834392D613363322D346438632D383164642D396131393939343765343764000000004200080100000038420 0
0A07000000044E616D6500000000042000B0100000020420053070000000044B65793100000000420052050000000400000
0010000000042000801000000 3042000A0700000013436F6E7461637420496E666F726D6174696F6E0000000000042000B
0700000003466F6F0000000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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:
```

Deleted: -0.98

Deleted: 28 September

```
    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


42007501000001604200740100000038420067010000002042006802000000040000000000000000420069020000000400
00000620000000042000D020000000400000002000000042000F0100000088420054A0500000004000000D0000000042
00900800000008290C75CAE59F39084200760100000060420091070000002437666261303834392D613363322D3464386
32D383164642D396131393939343765343764000000004200080100000028420004A070000000C782D6174747269627574
65310000000042000B070000000656616C756531000042000F0100000088420054A0500000004000000D0000000042009
00800000008BF48C307C95CC22E4200760100000060420091070000002437666261303834392D613363322D346438632D
383164642D396131393939343765343764000000004200080100000028420004A070000000C782D6174747269627574653
2000000042000B070000000656616C7565320000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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


42007801000001904200770100000048420067010000002042006802000000040000000000000000420069020000000400
00000620000000042008F090000000800000004AC07326420000D020000000400000002000000042000F01000009842
005A0500000004000000D0000000042009008000000008290C75CAE59F390842007C050000000400000000000000000420
```

Deleted: -0.98

Deleted: 28 September

	0790100000060420091070000002437666261303834392D613363322D346438632D383164642D39613139393934376534376400000000420008010000002842000A070000000C782D6174747269627574653100000000420000B070000000656616C7565310000042000F010000009842005A0500000004000000D0000000042009008000000008BF48C307C95CC22E42007C0500000004000000000000000042007901000000604200910700000024376662613038343920613633322D346438632D383164642D396131393939343765343764000000004200080100000028420000A070000000C782D6174747269627574653200000042000B070000000656616C7565320000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000001704200740100000038420067010000002042006802000000040000000000000004200690200000004000000620000000042000D020000000400000002000000042000F010000009042005A0500000004000000E000000004200900800000008A391110F7716FCFD42007601000000684200910700000024376662613038343920613633322D346438632D383164642D396131393939343765343764000000004200080100000028420000A070000000C782D6174747269627574653100000000420000B070000000E4D6F6469666965645661C756531000042000F010000009042005A0500000004000000E000000004200900800000008A391110F7716FCFD42007601000000684200910700000024376662613038343920613633322D346438632D383164642D396131393939343765343764000000004200080100000028420000A070000000C782D6174747269627574653200000042000B070000000E4D6F6469666965645661C7565320000 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:

Deleted: -0.98

Deleted: 28 September

```
      Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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


42007801000001A0420077010000004842006701000000204200680200000004000000000000000042006902000000040
0000006200000000042008F090000000800000004AC0732642000D020000000400000002000000004200 0F01000000A042
005A0500000004000000E000000004200900800000000842C6D3ED5BFE4F3442007C050000000400000000000000000420
079010000006842009107000000243766626130383439 2D613363322D346438632D383164642D396131393939343765 34
37640000000042000801000000 3042000A070000000C782D617474726962757465310000000042000B070000000E4D6F6
4696669656456616C756531000042000F01000000A042005A0500000004000000E000000004200900800000008A39111
0F7716FCFD42007C0500000004000000000000000004200790100000068420091070000002437666261303834392D61336
3322D346438632D383164642D396131393939343765343764000000004200080100000 3042000A070000000C782D6174
74726962757465320000000042000B070000000E4D6F64696669656456616C7565320000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

Deleted: -0.98

Deleted: 28 September

```
      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


42007501000001304200740100000038420067010000002042006802000000040000000000000000420069020000000400
00000620000000042000D020000000400000002000000042000F0100000070420005A0500000004000000F0000000042
00900800000008FB10B7D6A5F8F02F42007601000000484200910700000024376662613038343920D613363322D3464386
32D383164642D396131393939343765343764000000042000A0700000000C782D617474726962757465310000000042000
0F0100000070420005A0500000004000000F000000004200900800000008 3B5C2DE222A01A87420076010000004842009
1070000002437666261303834392D613363322D346438632D383164642D396131393939343765343764000000042000A
070000000C782D617474726962757465320000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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


42007801000001A042007701000000484200670100000020420068020000000400000000000000004200690200000004
00000062000000042008F090000000800000004AC0732742000D020000000400000002000000042000F01000000A042
005A0500000004000000F000000004200900800000008FB10B7D6A5F8F02F42007C0500000004000000F000000004200
07901000000684200910700000024376662613038343920D613363322D346438632D383164642D396131393939343765 34
```

Deleted: -0.98

Deleted: 28 September

<table>
<tr><td></td><td>37640000000042000801000000304200 0A070000000C782D61747472696275746531000000000042000B070000000E4D6F6
46966696564566 16C756531000042000F01000000A042005A0500000004000000 0F000000004200900800000000 83B5C2D
E222A01A8742007C050000000400000000000000004200790100000068420091070000002437666261303834392D61336
3322D346438632D383164642D39613139393934376534376400000000042000801000000304200 0A070000000C782D6174
7472696275746532000000000042000B070000000E4D6F6469666965645661 6C7565320000</td></tr>
<tr><td>8</td><td>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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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

42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400
00006200000000042000D0200000004000000010000000042000F01000000484200 5A0500000004000000140000000042
0076010000003042009107000000243766626130383439 2D613363322D346438632D383164642D396131393939343765 3
4376400000000

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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

420078010000000B04200770100000048420067010000002042006802000000040000000000000000420069020000000400
0000620000000042008F0900000008000000004AC0732742000D0200000004000000010000000042000F010000005842
005A0500000004000000140000000042007C05000000040000000000000000420079010000003042009107000000024376
66261303834392D613363322D346438632D383164642D39613139393934376534376400000000</td></tr>
<tr><td>9</td><td>Client A:
Get (symmetric key)
In: uuidKey</td></tr>
</table>

Deleted: -0.98

Deleted: 28 September

```
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400
00000620000000042000D020000000400000001000000042000F0100000048420 05A050000000400000000A0000000042
00760100000030420091070000002437666261303834392D613363322D346438632D383164642D3961313939393437653
4376400000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
42007801000000D042007701000000484200670100000020420068020000000400000000000000004200690200000004 0
00000062000000042008F090000000800000004AC0732742000D020000000400000001000000042000F010000007842
005A0500000004000000A0000000042007C0500000004000000010000000042007B0500000004000000010000000420
07A070000003A4E6F2043727970746F67726170686963204F626A65637420666F756E642077697468206769766 56E2055
6E697175652049646 56E74696669657200000000000
```

10	Client A: Destroy (template) In: uuidTemplate

```
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
```

Formatted: Swedish (Finland)

Deleted: -0.98

Deleted: 28 September

	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 42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400000006200000000042000D020000000400000001000000004200F01000000484200 5A05000000040000001400000000420076010000003042009107000000243833383331393862 2D343630302D343338382D393535662D3238303263633639396 5396300000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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: 8383198b-4600-4388-955f-2802cc699e9c 42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000000042008F090000000800000000 4AC0732742000D020000000400000001000000004200 0F010000005842005A05000000040000001400000000420076C05000000040000000000000000420079010000003042009107000000243833383331393862 2D343630302D343338382D393535662D3238303263633639396 5396300000000
11	Client A: Get (template) In: uuidTemplate 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400000006200000000042000D020000000400000001000000004200F01000000484200 5A0500000004000000A0000000042007601000000304200910700000024383338333139386 22D343630302D343338382D393535662D3238303263633639396

Deleted: -0.98

Deleted: 28 September

	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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```


```
42007801000000D042007701000000484200670100000020420068020000000400000000000000004200690200000004000000620000000042008F09000000080000000004AC0732742000D0200000004000000010000000042000F010000007842005A0500000004000000A0000000042007C0500000004000000010000000042007B0500000004000000010000000042007A070000003A4E6F2043727970746F677261706869632004F626A65637420666F756E6420776974682067697656E20556E6971756520496465E74696669657200000000000
```


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.

Deleted: ,

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 force the server to respond asynchronously, it is possible for a server to respond synchronously to the requests issued at times 1 and 4, in which case the expected response are the ones shown at times 2 and 5, respectively. In the case of the server not responding asynchronously to the Locate requests, the client is permitted to skip the requests illustrated at time 7 and 8.

Deleted: cannot

Deleted: may

Deleted: will be

Deleted: may be skipped by the client

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’ }

Deleted: -0.98

Deleted: 28 September

```
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
        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
```

```
420075010000019042007401000000384200670100000020420068020000000400000000000000004200690200000004000000620000000042000D020000000400000001000000042000F0100000148420050A0500000004000000010000000420076010000013042005505000000040000000200000000042008E0100000118420008010000003042000A0700000017437279707467726170686963204 16C676F726974686D0042000B05000000040000000300000000420008010000003042000A07000000144372797074 6F6772617068696320416C656E6774680000000042000B020000000400000080000000004200080100000038420 00A07000000144372797074 6F6772617068696320416C656E6774680000000042000B020000000400000080000000004200080100000038420 00A07000000044E616D650000000042000B0100000020420053070000000044B65793100000000420052050000000400000001000000004200080100000030420 00A0700000018437279707467726170686963205573616765204D61736B42000B020000000400000004000000042000801000000284200 0A0700000C4F626A6563742047726F75700000000042000B070000000647726F7570310000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
```

Deleted: -0.98

Deleted: 28 September

```
  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


42007801000000C0420077010000004842006701000000204200680200000004000000000000000042006902000000040
0000062000000042008F090000008000000004AC0781B42000D020000004000000010000000042000F010000006842
005A0500000004000000010000000042007C0500000004000000000000000042007901000000404200550500000004000
00002000000004200910700000024386239363132313312D393763372D343061362D383636342D656433333439316461623
56300000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)


42007501000000E042007401000000484200670100000020420068020000000400000000000000004200690200000004
0000006200000000420007060000000800000000000000142000D020000000400000001000000004200F010000008842
005A0500000004000000080000000042007601000000704200080100000002842000A070000000B4F626A6563742054797
065000000000042000B050000000400000002000000004200080100000003842000A07000000044E616D650000000042000
0B0100000020420053070000000044B65793100000000420052050000000400000001000000000


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: 0x00000000 (0)
```

Deleted: -0.98

Deleted: 28 September

```
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
420078010000008842007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000004200
8F090000000800000004AC0781C42000D020000000400000001000000004200
0F010000003042005A050000000400000008000000004200
7C050000000400000002000000004200
60800000008D1DE142AC6367B4B
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
420075010000007042007401000000384200670100000020420068020000000400000000000000004200690200000004000000062000000004200
2000F0100000028420050A050000000400000001A000000004200760100000010420060800000008D1DE142AC6367B4B
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004
```

Deleted: -0.98

Deleted: 28 September

	0000062000000004200 8F090000000800000000 4AC0781C42000D020000000400000001000000004200 0F010000005842005A0500000004000000080000000042007C0500000004000000000000000042007901000000304200910700000002438623936313231312D393763372D343061362D383636342D656433333439316461623563000000000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 420075010000009042007401000000384200670100000020420068020000000400000000000000004200690200000004000000062000000004200 0D020000000400000001000000004200 0F010000004842005A0500000004000000 0A00000000420076010000003042009107000000243862393631323131 2D393763372D343061362D383636342D656433333439316461623563000000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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)

Deleted: -0.98

Deleted: 28 September

	42007801000001204200770100000048420067010000002042006802000000040000000000000000042006902000000040000006200000000042008F090000000800000004AC0781D42000D020000000400000001000000042000F01000000C842005A0500000004000000A0000000042007C0500000004000000000000000042007901000000A042005505000000040000000020000000042009107000000243862393631323131 2D393763372D343061362D383636342D656433333439316461623563000000042008C01000000584200 3E010000005042004005000000040000000100000000420043010000001842004108000000010A1DF7B733D8DF7056623FE2D880EF62C42002605000000040000000300000000420028020000000400000008000000000
4	Client B: Locate (symmetric key by group) In: asynchronousIndicator='TRUE', attributes={ objectType = '00000002', 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000D042007401000000484200670100000020420068020000000400000000000000004200690200000004000000620000000042000706000000080000000000000014200 0D020000004000000010000000042000F010000007842005A0500000004000000080000000042007601000000604200080100000028420 00A070000000B4F626A6563742054797065000000000042000B050000000400000002000000004200080100000028420 00A070000000C4F626A6563742047726F757000000000042000B070000000647726F7570310000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007801000000884200770100000048420067010000002042006802000000040000000000000000042006902000000040

Deleted: -0.98

Deleted: 28 September

	0000062000000042008F0900000008000000004AC0781D42000D020000000400000001000000042000F010000003042 005A0500000004000000080000000042007C0500000004000000020000000420006080000000082DCF4F694617FC30
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000704200740100000038420067010000002042006802000000040000000000000000420069020000000400 0000062000000042000D020000000400000001000000042000F010000002842005A0500000040000001A0000000042 00760100000010420006080000000082DCF4F694617FC30 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004 0000006200000000042008F0900000008000000004AC0781D42000D020000000400000001000000042000F010000005842 005A0500000004000000080000000042007C0500000004000000000000000042007901000000304200910700000024386 23936313231312D393763372D343061362D383636342D656433333439316461623563000000000
6	Client B: Get (symmetric key) In: uuidKey2 Tag: Request Message (0x420075), Type: Structure (0x01), Data: Tag: Request Header (0x420074), Type: Structure (0x01), Data:

Deleted: -0.98

Deleted: 28 September

	Tag: Protocol Version (0x420067), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400000006200000000042000D020000000400000001000000042000F0100000048420005A0500000004000000A0000000042007601000000304200910700000024386239363132312D393763372D343061362D383636342D6564333334393164616235630000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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) 42007801000001204200770100000048420067010000002042006802000000040000000000000000420069020000000400000006200000000042008F090000000800000004AC0781D42000D020000000400000001000000042000F01000000C842005A0500000004000000A0000000042007C0500000004000000000000000042007901000000A042005505000000040000002000000004200910700000024386239363132312D393763372D343061362D383636342D6564333334393164616235630000000042008C010000005842003E0100000050420040050000000400000001000000004200430100000018420041080000001 0A1DF7B733D8DF7056623FE2D880EF62C42002605000000040000000300000000420028020000000400000008000000000
7	Client B: Locate (symmetric key by name) In: asynchronousIndicator='TRUE', attributes={ objectType = '00000002', Name= { Name='Key1',

Deleted: -0.98

Deleted: 28 September

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
```

```
42007501000000E0420074010000004842006701000000204200680200000004000000000000000042006902000000040
0000062000000004200070600000008000000000000000142000D020000000400000001000000042000F010000008842
005A0500000004000000080000000042007601000000704200080100000028420 00A07000000B4F626A6563742054797
065000000000042000B0500000004000000020000000042000801000000384200 0A07000000044E616D65000000004200
0B0100000020420053070000000 44B65793100000000420052050000000400000001000000 00
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
42007801000000884200770100000048420067010000002042006802000000040000000000000000420069020000000400
0000062000000042008F090000000800000004AC0781E42000D020000000400000001000000042000F010000003042
005A0500000004000000080000000042007C050000000400000002000000004200608000000008D48BDD01A8FFEC80
```

8	Client B: Cancel

Deleted: -0.98

Deleted: 28 September

	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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000704200740100000038420067010000002042006802000000040000000000000000420069020000000400000062000000000042000D020000000400000001000000042000F01000000284200 5A05000000040000001900000000420076010000000400000000000000042006902000000040000062000000000042000D020000000400000001000000042000F01000000284200760100000010420006080000000 8D48BDD01A8FFEC80 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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) 42007801000000A042007701000000484200670100000020420068020000000400000000000000004200690200000004000000620000000004200 8F090000000800000004AC0781F42000D020000000400000001000000042000F010000004842005A05000000040000001900000000420076C05000000040000000000000000042007901000000204200608000000 08D48BDD01A8FFEC8042001205000000040000000100000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
9	Client A: Destroy (symmetric key) In: uuidKey

Deleted: -0.98

Deleted: 28 September

```
  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


42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400
0000062000000004200D020000000400000001000000004200F01000000484200 5A0500000004000000140000000042
00760100000030420091070000002438623936313231312D393763372D343061362D383636342D65643333343931646162
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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: 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


42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000
0000062000000000042008F090000000800000004AC0781F42000D020000000400000001000000004200 0F010000005842
005A0500000004000000140000000042007C050000000400000000000000004200790100000030420091070000002438623
23936313231312D393763372D343061362D383636342D656433333439316461623563000000000
```

* = 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.

Deleted: the

Deleted: may or may not

Deleted: .

Time	Client A

Deleted: -0.98

Deleted: 28 September

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
```

```
42007501000001604200740100000038420067010000002042006802000000040000000000000000420069020000000400
00000620000000042000D020000000400000001000000042000F0100000118420054050000000400000001000000004200
76010000010042005505000000040000000220000000042008E01000000E842000801000000304200A0700000017437
27970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200
0A0700000014437279707 46F6772617068696320 4C656E67746800000000420 00B020000000400000080000000042000
80100000038420 0A07000000044E616D650000000042000B0100000020420053070000000 44B65793100000000420052
05000000040000001000000004200080100000030420 0A07000000184372797074 6F6772617068696320557361676520
04D61736B42000B020000000400000004000000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008F), Type: Date-Time (0x09), Data: 0x000000004AC0781F (Mon Sep 28
10:47:27 CEST 2009)
```

Deleted: -0.98

Deleted: 28 September

	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 42007801000000C0420077010000004842006701000000204200680200000004000000000000000042006902000000040000006200000000042008F090000000800000004AC0781F42000D020000000400000001000000042000F010000006842005A050000000400000001000000042007C050000000400000000000000042007901000000404200550500000004000000020000000042009107000000243333336463396239 2D386537332D346666362D613337622D34323336396635613432363200000000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000A042007401000000384200670100000020420068020000000400000000000000004200690200000004000000620000000042000D020000000400000001000000042000F01000000584200 5A05000000040000000B0000000420076010000004042009107000000243333336463396239 2D386537332D346666362D613337622D34323336396635613432363200000000042000A07000000055374617465000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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-

Deleted: -0.98

Deleted: 28 September

	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) 42007801000000D842007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000000042008F090000000800000004AC0782042000D020000000400000001000000004200F010000008042005A050000000400000000B0000000042007C050000000400000000000000004200790100000058420091070000002433333364633962392D386537332D346666362D613337622D343233363966356134323632000000004200080100000020420005A07000000055374617465000000420000B050000000400000001000000000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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) 42007501000000C042007401000000384200670100000020420068020000000400000000000000004200690200000004000000062000000000042000D020000000400000001000000004200F01000000784200 5A050000000400000000D0000000042007601000000604200910700000024333333646339623 92D386537332D346666362D613337622D343233363966356134323632000000004200080100000020420005A070000000F41637469766174696F6E20446174650042000B09000000080000000000000002 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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-

Deleted: -0.98

Deleted: 28 September

	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) 42007801000000E042007701000000484200670100000020420068020000000400000000000000004200690200000004000000620000000042008F090000000800000004AC0782042000D020000000400000001000000004200 0F010000008842005A050000000400000000D0000000042007C05000000040000000000000000420079010000006042009107000000243333336463396239 2D386537332D346666362D613337622D343233336396635613432363200000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B0900000008000000000000002
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000A042007401000000384200670100000020420068020000000400000000000000004200690200000004000000620000000042000D020000000400000001000000004200 0F01000000584200 5A050000000400000000B0000000042007601000000404200910700000024333333646339623 92D386537332D346666362D613337622D343233363966356134323632000000004200 8010000002842000A070000000055374617465000000 Out: uuidKey, attribute={ State='00000002' } 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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

Deleted: -0.98

Deleted: 28 September

	Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active) 42007801000000D84200770100000048420067010000002042006802000000040000000000000000042006902000000040 00000620000000042008F090000008000000004AC0782042000D020000000400000001000000042000F010000008042 005A0500000004000000B0000000042007C0500000004000000000000000042007901000000584200910700000024333 33364633962392D386537332D346666362D613337622D343233363966356134323632000000004200080100000020420 0A0700000005537461746500000042000B0500000004000000020000000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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) 42007501000000D042007401000000384200670100000020420068020000000400000000000000004200690200000004 00000062000000042000D020000000400000001000000042000F010000008842005A05000000040000000800000004 2007601000000704200080100000028420 00A070000000B4F626A6563742054797065000000000042000B0500000004000 00002000000004200080100000038420 00A07000000044E616D650000000042000B0100000020420053070000000044B65 7931000000004200520500000004000000010000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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:

Deleted: -0.98

Deleted: 28 September

	Tag: Unique Identifier (0x420091), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a4262 42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000004200 8F090000000800000004AC0782142000D020000000400000001000000004200 0F010000005842005A050000000400000008000000004200 7C050000000400000000000000004200 7901000000304200910700000024333333646339623 92D386537332D346666362D613337622D343233363966356134323632000000000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400 0000062000000004200 0D020000000400000001000000004200 0F010000004842005A050000000400000000A0000000042 00760100000030420091070000002433333364633962392D386537332D346666362D613337622D3432333639663561343 2363200000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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: E6C15B28BB6C7A268E9ADEA47IA36F23

Deleted: -0.98

Deleted: 28 September

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

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

```
42007801000001204200770100000048420067010000002042006802000000040000000000000000420069020000000400000062000000042008F090000000800000004AC0782142000D020000000400000001000000042000F01000000C842005A05000000040000000A0000000042007C05000000040000000000000000420079010000000A04200550500000004000000020000000042009107000000243333336463396239 2D386537332D346666362D613337622D343233363966356134323632000000042008C010000005842003E010000005042004005000000040000000100000000420043010000001842004108000000010E6C15B28BB6C7A268E9ADEA471A36F2342002605000000040000000300000000420028020000000400000008000000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
```

```
42007501000000B84200740100000038420067010000002042006802000000040000000000000000420069020000000400000062000000042000D020000000400000001000000042000F01000000 7042005A05000000040000001300000000420076010000058420091070000002433333364633962392D386537332D346666362D613337622D343233363966356134323632000000042007E010000001042007F05000000040000000200000000 42001F0900000008000000000000006
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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-
```

Deleted: -0.98

Deleted: 28 September

	42369f5a4262 42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000004200 8F090000000800000004AC0782242000D020000000400000001000000004200 0F010000005842005A0500000004000000130000000042007C05000000040000000000000000420079010000003042009107000000243333364633962392D386537332D346666362D613337622D343233363966356134323632000000000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000A042007401000000384200670100000020420068020000000400000000000000004200690200000004000000062000000004200 D020000000400000001000000004200 0F01000000584200 5A0500000004000000B000000004200 7C0500000004000000000000000004200 7901000000304200 9107000000243333336463396239 2D386537332D346666362D613337622D343233363966356134323632000000000 42000A07000000055374617465000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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) 42007801000000D842007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000004200 8F090000000800000004AC0782242000D020000000400000001000000004200 0F010000008042005A0500000004000000B000000004200 7C0500000004000000000000000004200 7901000000584200 9107000000024333

Deleted: -0.98

Deleted: 28 September

	33364633962392D386537332D346666362D613337622D343233363966356134323632000000004200080100000020420000A0700000005537461746500000042000B0500000004000000040000000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400000062000000004200D020000000400000001000000042000F01000000484200 5A05000000040000000C000000042007601000000304200910700000024333333646339623 92D386537332D346666362D613337622D3432333639663561343236320000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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

Deleted: -0.98

Deleted: 28 September

	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 42007801000002284200770100000048420067010000002042006802000000040000000000000000420069020000000400000062000000042008F090000000800000004AC0782242000D020000000400000001000000042000F01000001D042005A0500000004000000C0000000042007C0500000004000000000000000042007901000001A842009107000000243333364633962392D386537332D346666362D613337622D343233363966356134323632000000042000A07000000144372797074 6F6772617068696320455736167652040617465000000042000A070000001A436F6D70726F6D697365204F6363757272656E6365204461746500000000000042000A070000000F436F6D70726F6D6973652044617465004200 0A07000000064469676573747400004200A070000000C496E697469616C204461746500000000042000A070000000F41637469766174696F6E2044617465004200A07000000011526576F636174696F6E20526561736F6E000000000000000042000A0700000011556E697165204964656E74696669657200000000000000042000A07000000044E616D650000000042000A07000001843727970746F6772617068696320557361676520 4D61736B42000A070000000B4F626A65637420547970650000000000042000A07000000114C617374204368616E67656420446174650000000000000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000000A042007401000000384200670100000020420068020000000400000000000000004200690200000004000000620000000042000D020000000400000001000000042000F0100000058420005A0500000004000000B0000000042007601000000404200910700000024333333646339623 92D386537332D346666362D613337622D3432333639663561343236320000000042000A07000000055374617465000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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-

Deleted: -0.98

Deleted: 28 September

	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) 42007801000000D84200770100000048420067010000002042006802000000040000000000000004200690200000004000000062000000042008F090000000800000004AC0782242000D020000000400000001000000042000F010000008042005A0500000004000000B0000000042007C0500000004000000000000000042007901000000584200910700000024333333646339623 92D386537332D346666362D613337622D343233363966356134323632000000004200080100000020420000A0700000005537461746500000042000B0500000004000000040000000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000001604200740100000038420067010000002042006802000000040000000000000004200690200000004000000062000000042000D020000000400000002000000004200 0F010000008842005A0500000004000000D0000000042009008000000085CD7C98FC5B52FF74200760100000060420091070000002433333364633962392D386537332D346666362D613337622D343233363966356134323632000000004200080100000020420000A070000000C782D6174747269627574653100000000042000B070000000656616C756531000042000F010000008842005A0500000004000000D0000000042009008000000008F0CB35D89BB9D2514200760100000060420091070000002433333364633962392D386537332D346666362D613337622D343233363966356134323632000000004200080100000020420000A070000000C782D6174747269627574653200000000042000B070000000656616C7565320000 Out: uuidKey, attribute={ x-attribute1='Value1' } Out: uuidKey, attribute={ x-attribute2='Value2' }

Deleted: -0.98

Deleted: 28 September

```
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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


42007801000001904200770100000048420067010000002042006802000000040000000000000000420069020000000400
0000062000000042008F090000000800000004AC0782342000D020000000400000002000000042000F010000009842
005A05000000040000000D0000000042009008000000085CD7C98FC5B52FF742007C05000000040000000000000000420
079010000006042009107000000243333336463396239 2D386537332D346666362D613337622D343233363963563413432
3632000000004200080100000028420 00A070000000C782D617474726962757465310000000042000B070000000656616
C756531000042000F01000000984200 5A05000000040000000D0000000042009008000000008F0CB35D89BB9D25142007C
0500000004000000000000000000420079010000006042009107000000243333336463396239 2D386537332D346666362D6
13337622D343233363966356134323632000000004200080100000028420 00A070000000C782D617474726962757465320
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
```

Deleted: -0.98

Deleted: 28 September

```
    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


42007501000001704200740100000038420067010000002042006802000000040000000000000000420069020000000400
00000620000000042000D020000000400000002000000042000F01000000904200 5A0500000040000000E0000000042
00900800000008C06597C23C952144420076010000006842009107000000243333336463396239 2D386537332D3466663
62D613337622D343233363966356134323632000000004200080100000030420 00A070000000C782D6174747269627574
653100000000042000B070000000E4D6F6469666965645661 6C756531000042000F01000000904200 5A050000000400000
00E000000004200900800000008 3D9CF6E0445252B84200760100000068420091070000002433333364633962392D3865
37332D346666362D613337622D343233363966356134323632000000004200080100000030420 00A070000000C782D617
4747269627574653200000000042000B070000000E4D6F6469666965645661 6C7565320000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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: 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)
```

Deleted: -0.98

Deleted: 28 September

	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 42007801000001A042007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000004200 8F090000000800000004AC0782342000D020000000400000002000000004200 0F01000000A042005A0500000004000000 0E000000004200900800000008C06597C23C95214442007C0500000004000000000000000042007901000000684200910700000024333333646339623923863732D346666362D613337622D343233336396356134323632000000004200080100000030420 00A070000000C782D6174746726962757465310000000042000B070000000E4D6F64696696564566 16C756531000042000F01000000A042005A0500000004000000 0E000000004200900800000083D9CF6E0445252B842007C0500000004000000000000000042007901000000684200910700000024333333646339623923863732D346666362D613337622D343233336396356134323632000000004200080100000030420 00A070000000C782D6174746726962757465320000000042000B070000000E4D6F64696696564566 16C7565320000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007501000001304200740100000038420067010000002042006802000000040000000000000000420069020000000400000062000000004200D020000000400000002000000004200 0F01000000704200 5A0500000004000000 0F000000004200900800000008B77FD0753B7C95ED420076010000004842009107000000243333336463396235 62D343233363966356134323632000000004200 0A070000000C782D6174726962757465320000000042000A070000000C782D6174726962757465320000000042000A070000000C782D6174726962757465320000000 Out: uuidKey, attributeNames={ 'x-attribute1' } Out: uuidKey, attributeNames={ 'x-attribute2' }

Deleted: -0.98

Deleted: 28 September

```
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
42007801000001A042007701000000484200670100000020420068020000000400000000000000004200690200000004000000620000000042008F090000000800000004AC0782642000D020000000400000002000000004200 0F01000000A042005A05000000040000000F000000004200900800000081A1B48172DF57ABC42007C05000000040000000000000000420079010000006842009107000000024333333646339623 92D386537332D346666362D613337622D343233363963563413432363200000000420008010000003042000A070000000C782D6174747269627574653100000000420 00B070000000E4D6F64696669656456616C756531000042000F01000000A042005A05000000040000000F000000004200900800000008B77FD0753B7C95ED42007C0500000004000000000000000004200790100000068420091070000002433333364633962392D386537332D346666362D613337622D343233363966356134323632000000004200080100000030420 00A070000000C782D617474726962757465310000000042000B070000000E4D6F64696669656456616C7565320000042000B070000000E4D6F64696669656456616C7565320000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
```

Deleted: -0.98

Deleted: 28 September

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


42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400
0000062000000004200D020000000400000001000000004200F01000000484200 5A0500000004000000A0000000042
00760100000030420091070000002433333364633962392D386537332D346666362D613337622D34323333639663561343
2363200000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)


420078010000012042007701000000484200670100000020420068020000000400000000000000004200690200000004
0000006200000000042008F090000000800000004AC0782742000D020000000400000001000000004200 0F01000000C842
005A0500000004000000A0000000042007C0500000004000000000000000042007901000000A042005505000000040000
0000200000000042009107000000243333336463396239 2D386537332D346666362D613337622D343233363966356134323
6320000000042008C010000005842003E0100000050420040050000000400000001000000004200430100000001842004
10800000010E6C15B28BB6C7A268E9ADEA471A36F2342002605000000040000000300000000420028020000000400000
8000000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
```

Deleted: -0.98

Deleted: 28 September

```
    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


42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400
0000062000000004200D020000000400000001000000004200F01000000484200 5A05000000040000001400000000420
0076010000003042009107000000243333336463396239 2D386537332D346666362D613337622D3432333639663561343
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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


42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004
0000006200000000042008F090000000800000004AC0782742000D020000000400000001000000004200 0F010000005842
005A05000000040000001400000000420 07C05000000040000000000000000420079010000003042009107000000243333
33646339623 92D386537332D346666362D613337622D343233363966356134323632000000000
```

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:

Formatted: English (U.S.)

Deleted: -0.98

Deleted: 28 September

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
```

```
42007501000001604200740100000038420067010000002042006802000000040000000000000000420069020000000400
00006200000000420000D020000000400000001000000004200F010000011842005A0500000004000000010000000042000
760100000100420055050000000400000002000000004200 8E01000000E84200080100000030420000A0700000017437279
70746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200 0A07
0000001443727970746F6772617068696320 4C656E6774680000000042000B020000000400000080000000004200080100
00003842000A07000000044E616D650000000042000B01000000204200530700000004 4B65793100000000420052050000
0004000000010000000042000801000000304200 0A0700000018437279707 46F6772617068696320557361676520 4D6173
6B42000B020000000400000004000000 00
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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:
```

Formatted: English (U.S.)

Deleted: -0.98

Deleted: 28 September

	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 42007801000000C042007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000004200 8F0900000008000000004AC0782842000D020000000400000001000000004200 0F01000000684200 5A0500000004000000010000000042007C0500000004000000000000000042007901000000404200550500000004000000020000000042009107000000243466656336135392D623231372D346162662D383461642D6166313534373032343631350000000042007C0500000004000000000000000042007901000000404200550500000004000000020000000042009107000000243466656336135392D623231372D346162662D383461642D616631353437303234363135000000004AC07A80
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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) 42007501000001684200740100000038420067010000002042006802000000040000000000000000420069020000000400000062000000004200 0D020000000400000002000000004200 0F01000000884200 5A0500000004000000 0D000000004200 900800000008E1AE8A5206CC749A42007601000000604200910700000024346665633361353 92D623231372D346162662D383461642D616631353437303234363135000000004200 0801000000284200 0A070000000F41637469766174696F6E2044617465004200 0B090000000800000000000000000242000F01000000904200 5A0500000004000000 0D000000004200 900800000008C6CAA6E0C409336F42007601000000684200910700000024346665633361353 92D623231372D346162662D383461642D616631353437303234363135000000004200 0801000000304200 0A070000001150726F746563742053746F7020446174650000000000000042000B090000000800000004AC07A80

Deleted: -0.98

Deleted: 28 September

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
```

```
42007801000001984200770100000048420067010000002042006802000000040000000000000000420069020000000400
0000062000000042008F090000000800000004AC0782842000D020000000400000002000000042000F01000000984200
5A0500000004000000D0000000042009008000000008E1AE8A5206CC749A42007C050000000400000000000000000420079
0100000060420091070000002434666563336135392D623231372D346162662D383461642D6166313534373032343631350000000042000801000002842000A07000000F41637469766174696F6E2044617465004200B0900000008000000000000000242000F01000000A042005A0500000004000000D0000000042009008000000008C6CAA6E0C409336F42007C0500000004000000000000000042007901000000684200910700000024346665633361353920D623231372D346162662D383461642D6166313534373032343631350000000042000801000000304200A07000000115072F746563742053746F7020446174650000000000000042000B0900000008000000004AC07A80
```

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: 0x00000000 (0)
```

Deleted: -0.98

Deleted: 28 September

Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)

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)

```
4200750100000C84200740100000038420067010000002042006802000000040000000000000000420069020000000400
0000062000000004200D020000000400000001000000042000F010000008042005A050000000400000000D000000004200
760100000068420091070000002434666563336135392D623231372D346162662D383461642D616631353437303234363135
350000000042000801000000342000A070000000C5573616765204C696D6974730000000042000B010000001042009504
0000000800000000000003E8
```

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: 0x00000000 (0)

Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)

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)

```
4200780100000F84200770100000048420067010000002042006802000000040000000000000000420069020000000400
0000062000000004200 8F090000000800000000 4AC0782A42000D020000000400000001000000042000F01000000A04200
5A050000000400000000D000000042007C050000000400000000000000004200790100000078420091070000002434666 5
63336135392D623231372D346162662D383461642D616631353437303234363135000000004200080100000042000A07
0000000C5573616765204C696D6974730000000042000B010000002042009504000000080000000000003E84200930400
0000080000000000003E8
```

3 Client B:

Locate (symmetric key by name)

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

Deleted: -0.98

Deleted: 28 September

```
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
```

```
4200750100000D042007401000000384200670100000020420068020000000400000000000000004200690200000004000
00006200000000042000D020000000400000001000000004200F010000008842005A0500000004000000080000000042000
760100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000
020000000042000801000000384200A07000000044E616D650000000042000B01000000204200530700000044B657931
000000004200520500000004000000010000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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: 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
```

```
4200780100000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000
00006200000000042008F090000000800000004AC0782A42000D020000000400000001000000004200F01000000584200
5A0500000004000000080000000042007C0500000004000000000000000042007901000000304200910700000024346665
63336135392D623231372D346162662D383461642D616631353437303234363135000000000
```

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

Formatted: English (U.S.)

Deleted: -0.98

Deleted: 28 September

```
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400
0000620000000042000D020000000400000001000000042000F010000004842005A050000000400000000A000000004200
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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: 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)
```

```
42007801000001204200770100000048420067010000002042006802000000040000000000000000420069020000000400
0000620000000042008F090000000800000004AC0782A42000D020000000400000001000000042000F01000000C84200
5A0500000004000000A0000000042007C0500000004000000000000000042007901000000A042005050000000040000000
0200000000420091070000002434666563336135392D623231372D346162662D383461642D6166313534373032343631350
0000000042008C010000005842003E0100000050420040050000000400000001000000004200430100000018420041080
0000103D41DF1C5C20E272212D86D762A8C7D4420026050000000400000003000000004200280200000004000000800000
0000
```

5	Client B:

Deleted: -0.98

Deleted: 28 September

	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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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) 4200750100000A042007401000000384200670100000020420068020000000400000000000000004200690200000004000000620000000042000D020000000400000001000000004200F01000000584200576010000004042009107000000243466656336135392D623231372D346162662D383461642D6166313534373032343631350000000042009304000000080000000000001F4 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 4200780100000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000000620000000042008F090000000800000004AC0782A42000D020000000400000001000000004200F01000000584200A05000000040000001100000000420070500000004000000000000000042007901000000304200910700000024346665633361353920D623231372D346162662D383461642D6166313534373032343631350000000042009304000000080000000000001F4 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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
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:

Formatted: English (U.S.)

Deleted: -0.98

Deleted: 28 September

```
      Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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)
```

```
42007501000000A042007401000000384200670100000020420068020000000400000000000000004200690200000004000
00006200000000042000D020000000400000001000000004200F010000005842005A05000000040000001100000000420007
601000000404200910700000024346665633361353 92D623231372D346162662D383461642D6166313534373032343631
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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000
00006200000000042008F0900000008000000004AC0782B42000D020000000400000001000000004200 0F01000000584200
5A05000000040000001100000000420 07C05000000040000000000000000420079010000003042009107000000243466656
63336135392D623231372D346162662D383461642D6166313534373032343631350000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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:
```

Formatted: English (U.S.)

Deleted: -0.98

Deleted: 28 September

```
        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)
```

```
42007501000000D042007401000000384200670100000020420068020000000400000000000000004200690200000004000
00006200000000042000D020000000400000001000000004200F01000000884200 5A0500000004000000080000000042000
760100000070420008010000002842000A07000000B4F626A656374205479706500000000042000B0500000004000000
020000000042000801000000384200 0A07000000044E616D650000000042000B01000000204200530700000044B657931
000000004200520500000004000000010000000 0
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000
00006200000000042008F090000000800000004AC0782B42000D020000000400000001000000004200 0F01000000584200
5A0500000004000000080000000042007C0500000004000000000000000042007901000000304200910700000024346665
63336135392D623231372D346162662D383461642D6166313534373032343631350000000 0
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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-
```

Formatted: English (U.S.)

Deleted: -0.98

Deleted: 28 September

	af1547024615 42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400000062000000004200D020000000400000001000000042000F0100000048420 05A05000000040000000A000000004200760100000030420091070000002434666563336135392D623231372D346162662D383461642D6166313534373032343631350000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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) 42007801000001204200770100000048420067010000002042006802000000040000000000000000420069020000000400000062000000004200 8F090000000800000004AC0782B42000D020000000400000001000000042000F01000000C842005A0500000004000000A0000000042007C0500000004000000000000000042007901000000A042005505000000040000002000000004200910700000024346665633361353 92D623231372D346162662D383461642D6166313534373032343631350000000042008C01000000584200 3E0100000050420040050000000400000001000000004200430100000018420041080000000103D41DF1C5C20E272212D86D762A8C7D4420026050000000400000003000000004200280200000004000008000000000 Out: uuidKey, UsageLimitsByteCount='500'
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

Deleted: -0.98

Deleted: 28 September

```
  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)
```

```
42007501000000A042007401000000384200670100000020420068020000000400000000000000004200690200000004000
0000620000000042000D020000000400000001000000042000F0100000058420050A0500000004000000110000000042000
760100000040420091070000002434666563336135392D623231372D346162662D383461642D6166313534373032343631
350000000042009304000000080000000000001F4
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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: 0x00000001 (Failed)
    Tag: Result Reason (0x42007B), Type: Enumeration (0x05), Data: 0x0000000C (Permission Denied)
    Tag: Result Message (0x42007A), Type: Text String (0x07), Data: Unable to allocate requested
byte amount
```

```
42007801000000B842007701000000484200670100000020420068020000000400000000000000004200690200000004000
0000620000000042008F0900000008000000004AC0782B42000D020000000400000001000000042000F01000000604200
5A0500000004000000110000000042007C0500000004000000010000000042007B0500000004000000C0000000042007A
0700000028556E61626C6520746F20616C6C6F6361746520726571756573746564206279746520616D6F756E74
```

10

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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: 4fec3a59-b217-4abf-84ad-
af1547024615
```

```
42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400
0000620000000042000D020000000400000001000000042000F0100000048420050A0500000004000000140000000042000
```

Formatted: English (U.S.)

Deleted: -0.98

Deleted: 28 September

```
760100000030420091070000002434666563336135392D623231372D346162662D383461642D6166313534373032343631
3500000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000
0000620000000042008F090000000800000004AC0782C42000D020000000400000001000000042000F01000000584200
5A0500000004000000140000000042007C050000000400000000000000004200790100000030420091070000002434666565
63336135392D623231372D346162662D383461642D6166313534373032343631350000000
```

6 Key Interchange, Key Exchange

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

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

Time	Request/Response messages

0	Register (symmetric key)
	In: objectType = '00000002', attributes={ CryptographicUsageMask='00000004' }, foreignSymmetricKey
	
	`Tag: Request Message (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: 0x00000000 (0)`
	`  Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)`
	`  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:`

Formatted: English (U.S.)

Deleted: -0.98

Deleted: 28 September

```
    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
Mask
          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)
```

```
42007501000001104200740100000038420067010000002042006802000000040000000000000000420069020000000400000062000000004200
0D020000000400000001000000004200
0F01000000C842005A0500000004000000030000000420076010000
00B042005505000000040000000200000000042008E01000000384200080100000030420
00A0700000018437279707466F6772617068696320557361676520
4D61736B42000B020000000400000004000000004200
8C01000000584200
3E0100000050420040050000000400000001000000004200430100000018420041080000001001234567
89ABCDEF0123456789ABCDEF4200260500000004000000030000000042002802000000040000008000000000
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000000620000000042008F09000000080000000004AC0782C42000D020000000400000001000000004200
0F010000005842005A0500000004000000030000000042007C0500000004000000000000000042007901000000304200910700000024626238303634353
32D356337352D343263322D383062642D346535326631636562353762000000000
```

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

Deleted: -0.98

Deleted: 28 September

```
      Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
420075010000000C042007401000000384200670100000020420068020000000400000000000000004200690200000004000000062000000004200
0D020000000400000001000000042000F0100000078420054050000000400000000D000000004200760100000060420091070000002462623830363435332D356337352D343263322D383062642D34653532663163656235376200000000420008010000002842000A070000000A782D70726F7669646572000000000000042000B0700000007756E6B6E6F776E00
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
    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
```

```
420078010000000E042007701000000484200670100000020420068020000000400000000000000004200690200000004000000062000000004200
8F090000000800000004AC0782E42000D020000000400000001000000042000F010000008842005A050000000400000000D000000004200790100000060420091070000002462623830363435332D356337352D343263322D383062642D34653532663163656235376200000000420008010000002842000A070000000A782D70726F7669646572000000000000042000B0700000007756E6B6E6F776E00
```

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: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)
```

Deleted: -0.98

Deleted: 28 September

	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 42007501000000C84200740100000038420067010000002042006802000000040000000000000000420069020000000400000006200000000042000D020000000400000001000000042000F0100000080420054050000000400000000E000000004200760100000068420091070000002462623830363435332D356337352D343263322D383062642D34653532663163656235376200000000420008010000003042000A070000000A782D70726F7669646572000000000000042000B070000000B74686972642070617274790000000000 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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) 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 42007801000000E84200770100000048420067010000002042006802000000040000000000000000420069020000000400000006200000000042008F090000000800000004AC0782E42000D020000000400000001000000042000F010000009042005A05000000040000000E0000000042007C05000000040000000000000000420079010000006842009107000000246262383036343533 2D356337352D343263322D383062642D34653532663163656235376200000000420008010000003042000A070000000A782D70726F7669646572000000000000042000B070000000B7468697264207061727479000000000
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: 0x00000000 (0) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Deleted: -0.98

Deleted: 28 September

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

```
42007501000000904200740100000038420067010000002042006802000000040000000000000000420069020000000400000062000000004200
0D020000000400000001000000004200F010000004842005A05000000040000001400000000420076010000003042009107000000246262383036
3435332D356337352D343263322D383062642D34653532663163656235376200000000
```

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: 0x00000000 (0)

Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000062 (98)

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

```
42007801000000B042007701000000484200670100000020420068020000000400000000000000004200690200000004000000620000000042008F
090000000800000004AC0782E42000D020000000400000001000000004200F010000005842005A05000000040000001400000000420070C050000
0004000000000000000042007901000000304200910700000024626238303634353 32D356337352D343263322D383062642D34653532663163656235376200000000
```

Formatted: English (U.S.)

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',

Deleted: -0.98

Deleted: 28 September

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

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

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

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

8 Asymmetric keys

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

8.1 Use-case: Create a Key Pair

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

Time	Client A
0	Create Key Pair In: commonAttributes={ CryptographicAlgorithm='RSA', CryptographicLength='1024', CryptographicUsageMask='0000000C' }, privateKeyAttributes={ Name={ NameValue='PrivateKey1', NameType='00000001' } }, publicKeyAttributes={ NameValue='PublicKey1', NameType='00000001' } }

Deleted: -0.98

Deleted: 28 September

	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 } }

Deleted: -0.98

Deleted: 28 September

	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.

Deleted: can

Deleted: be

Deleted: ed

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)

Deleted: -0.98

Deleted: 28 September

	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.

Deleted: should be

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

Deleted: -0.98

Deleted: 28 September

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

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.

Deleted: will

Time	Client A
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 Attribute In: uuidKey, attributeName={‘State’} Out: uuidKey, attribute={ State=‘*Active*’ }
2	Revoke (symmetric key as compromised) In: uuidKey, RevocationReason=’00000002’, CompromiseOccurrenceDate=’6’ Out: uuidKey
3	Get Attribute In: uuidKey, attributeName={‘State’} Out: uuidKey, attribute={ State=‘*Compromised*’ }
4	Rekey In: uuidKey, offset=’0’ Out: uuidNewKey

Deleted: -0.98

Deleted: 28 September

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

Deleted: -0.98

Deleted: 28 September

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	

Deleted: -0.98

Deleted: 28 September

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.

Deleted: The
Deleted: may be performed
Deleted: in which case
Deleted: must
Deleted: must also

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.

Deleted: should
Deleted: that
Deleted: should

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)

Deleted: -0.98
Deleted: 28 September

	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

Deleted: -0.98

Deleted: 28 September

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:

TBD

Deleted: -0.98

Deleted: 28 September

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.
ed-0.98	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

Deleted: -0.98

Deleted: 28 September