TBD (Key Management Interoperability Protocol Use Cases)

Editor's Draft 0.98

6 August 2009

Deleted: 28 April

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

Deleted: Robert Haas

Related work:
This specification replaces or supersedes:

- None

This specification is related to:

- TBD

Declared XML Namespace(s):
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.

Deleted: 28 April

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

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

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

Deleted: 28 April

Notices

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

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

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

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

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

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

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

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

Deleted: 28 April

Table of Contents

Deleted: 28 April

1 Introduction

The purpose of this document is to describe use-cases to demonstrate the Key Management Interoperability Protocol (KMIP). The use-cases shall indicate if all concepts within the protocol are sound and can be used to implement 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. the attribute index may or may not be omitted if it is zero). Also note that many values will 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 Document Roadmap

TBD

1.2 Goals and Requirements

TBD

1.3 Notational Conventions

TBD

1.4 Namespaces

TBD

1.5 Terminology

TBD

1.6 Normative References

TBD

1.7 Non-normative References

TBD

1.8 Compliance

TBD

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Deleted: 28 April

2 Message exchange

The message exchange between clients and the server to test the following use-case scenarios shall happen 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' } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x42008D), 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) 420073010000012042007201000000384200650100000020420066020000000400000000000000004200670200000004

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Deleted: i

Deleted: s

Formatted: Indent: Left: 0 pt

Deleted: creation

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Normal, No bullets or numbering

Formatted: Font: 10 pt, Font color: Auto

Deleted: 12

Deleted: 28 April

	0000006200000000042000D0200000004000000010000000042000F01000000D84200570500000004000000010000000042007401000000C0420052050000000400000002000000042008D01000000A84200080100000030420008A0700000014437279707465772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000342000A0700000014437279707465772617068696320416C656E6774680000000042000B020000000400000080000000042000801000000342000A0700000018437279707465772617068696320557361676520 4D61736B42000B0200000004 0000000C00000000 Out: objectType='00000002', uuidKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8E7 (Thu Jul 30 17:14:47 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 77b971bc-a932-43ba-8f1b-81191f529ab9 42007601000000C0420075010000004842006501000000204200660200000004000000000000000042006702000000040000006200000000042008E090000000800000004A71B8E742000D020000000400000001000000042000F0100000006842005705000000040000000100000000042007A05000000040000000000000000420077010000004042005205000000040000006200000000042008F0700000024373762393731626 32D613933322D343362612D386631622D3831313931663532 3961623900000000
1	Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 77b971bc-a932-43ba-8f1b-81191f529ab9 42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000004 0000006200000000042000D0200000004000000010000000042000F0100000048420057050000000400000014000000004200740100000003042008F0700000024373762393731626 32D613933322D343362612D386631622D3831313931663532 3961623900000000 Out: uuidKey

Deleted: 28 April

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8E8 (Thu Jul 30
17:14:48 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 77b971bc-a932-43ba-
8f1b-81191f529ab9


42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000004
00000062000000042008E090000000800000004A71B8E842000D020000000400000001000000042000F0100000058
42005705000000040000001400000000042007A050000000400000000000000004200770100000003042008F0700000024
3737623937316263 2D613933322D343362612D386631622D383131393166353239616239000000 00
```

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.

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Normal, No bullets or numbering

Formatted: Default Paragraph Font, Font color: Auto

Time	Request/Response messages
0	Register (template) In: objectType='00000007', attributes={ ObjectGroup='Group1', ApplicationSpecificID='ssl, www.example.com', ContactInformation='Joe', x-Purpose='demonstration', Name={ NameValue='Template1', NameType='00000001' } }

Deleted: templateName = 'Template1',

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000003 (Register)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000006 (Template)
      Tag: Template-Attribute (0x42008D), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group
```

Deleted: 28 April

```
          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
Identification
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Application Name Space (0x420003), Type: Text String (0x07), Data: ssl
            Tag: Application Identifier (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 (0x420050), Type: Text String (0x07), Data: Template1
            Tag: Name Type (0x42004F), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)


42007301000001C84200720100000038420065010000002042006602000000040000000000000000420067020000000400
00000620000000042000D020000000400000001000000042000F0100000180420057050000000400000003000000004200
74010000016842005205000000040000000600000000042008D0100000150420008010000002842000A070000000C4F6
26A6563742047726F75700000000042000B0700000006477 26F75703100004200080100000006042000A07000000234170
706C69636174696F6E2053706563696669632049646 56E74696669636174696F6E000000000042000B010000002842000
3070000000373736C000000000042000207000000 0F7777772E6578616D706C652E636F6D0042000801000000304200 0A
0700000013436F6E7461637420496E666F726D6174696F6E000000000042000B07000000034A6F650000000000042000800
10000003042000A0700000009782D507572706F7365000000000000000042000B070000000D64656D6F6E7374726174696F
6E000000420008010000004042000A07000000044E616D650000000042000B0100000028420050070000000954656D706
C617465310000000000000042004F0500000004000000100000000
```

Out: objectType='00000007', uuidTemplate

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8E9 (Thu Jul 30
17:14:49 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000003 (Register)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000006 (Template)
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 80a5be03-1d2b-4190-917e-
34ed82a661b8


42007601000000C042007501000000484200650100000020420066020000000400000000000000004200670200000004000
00006200000000042008E090000000800000004A71B8E942000D020000000400000001000000004200 0F010000006842
00570500000004000000030000000042007A0500000004000000000000000042007701000000404200520500000004000
00006000000004200 8F07000000243830613562653033 2D316432622D343139302D393137652D333465643832613636 31
```

Deleted: 28 April

	623800000000
1	Create (symmetric key using template) In: objectType='00000002', template={ NameValue='Template1', NameType='00000001' }, attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C' }

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x42008D), Type: Structure (0x01), Data:
        Tag: Name (0x42004E), Type: Structure (0x01), Data:
          Tag: Name Value (0x420050), Type: Text String (0x07), Data: Template1
          Tag: Name Type (0x42004F), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt,
Decrypt)


42007301000001504200720100000038420065010000002042006602000000040000000000000000420067020000000400
00000620000000042000D020000000400000001000000004200F0100000108420057050000000400000001000000004200
7401000000F042005205000000040000000200000000042008D01000000D842004E010000002842005007000000095465
56D706C617465310000000000000042004F0500000004000000010000000042000801000000304200A07000000174372
7970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200
A0700000014437279707 46F6772617068696320 4C656E6774680000000042000B020000000400000080000000004200080
10000003042000A0700000018437279707 46F6772617068696320557361676520 4D61736B42000B020000000400000000
C00000000
```

Out: objectType='00000002', uuidKey

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8E9 (Thu Jul 30
17:14:49 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
```

Deleted: ¶

Deleted: 12

Deleted: 28 April

```
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 0c24f92a-658a-464a-8964-
096acea02cd8


42007601000000C042007501000000484200650100000020420066020000000400000000000000004200670200000004
0000006200000000042008E090000000800000004A71B8E942000D020000000400000001000000004200 0F010000006842
00570500000004000000010000000042007A05000000040000000000000004200770100000040420052050000000400
0000200000000042008F0700000024306332346639326 12D363538612D343634612D383936342D3039366163656130326 3
643800000000
```

2 Get attributes

In: uuidKey, attributeNames={‘ObjectGroup’, ‘ApplicationSpecificID’, ‘ContactInformation’, ‘x-Purpose’}

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 0c24f92a-658a-464a-8964-
096acea02cd8
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Application Specific
Identification
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-Purpose


42007301000001104200720100000038420065010000002042006602000000040000000000000000420067020000000400
0000062000000004200 0D020000004000000010000000042000F01000000C842005705000000040000000B00000000042
007401000000B042008F0700000024306332346639326 12D363538612D343634612D383936342D3039366163656130326
364380000000042000A070000000C4F626A6563742047726F757000000000042000A0700000023417070 6C69636174696F
6E20537065636966696320496 4656E7469666963617469 6F6E000000000042000A0700000013436F6E7461637420496E6
66F726D6174696F6E00000000042000A0700000009782D507572706F736500000000000000
```

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

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8EA (Thu Jul 30
17:14:50 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
```

Deleted: 28 April

	Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 0c24f92a-658a-464a-8964-096acea02cd8 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 Identification Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Application Name Space (0x420003), Type: Text String (0x07), Data: ssl Tag: Application Identifier (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 42007601000001B84200750100000048420065010000002042006602000000040000000000000000042006702000000040000006200000000042008E090000000800000004A71B8EA42000D020000000400000001000000004200 0F010000016042005705000000004000000B0000000042007A05000000040000000000000000420077010000013842008F0700000024306 33234663932612D363538612D343634612D383936342D303936616365613032636438000000004200080100000028420008A070000000C4F626A6563742047726F757000000000042000B07000000064772 6F757031000042000801000000604200 0A070000000C4F626A6563742047726F757000000000042000B07000000064772 6F757031000042000801000000604200 A07000000234170706C69636174696F6E20537065636966696320496 4656E74696669636174696F6E000000000042000B 0100000028420003070000000373736C000000000042000207000000 0F7777772E6578616D706C652E636F6D004200080 10000003042000A0700000013436F6E7461637420496E666F726D6174696F6E000000000042000B07000000034A6F6500 0000000042000801000000 3042000A0700000009782D507572706F736500000000000000042000B070000000D64656D6F6 E7374726174696F6E000000
3	Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 0c24f92a-658a-464a-8964-096acea02cd8 42007301000000904200720100000038420065010000002042006602000000040000000000000000042006702000000040000006200000000042000D020000000400000001000000004200F010000004842005705000000040000001400000000420074010000003042008F0700000024306332346639326 12D363538612D343634612D383936342D303936616365613032636438000000 Out: uuidKey

Deleted: 28 April

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8EA (Thu Jul 30
17:14:50 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 0c24f92a-658a-464a-8964-
096acea02cd8
```

```
42007601000000B042007501000000484200650100000020420066020000000400000000000000000420067020000000400
00000620000000042008E090000000800000004A71B8EA42000D020000000400000001000000004200 0F010000005842
00570500000004000000140000000042007A050000000400000000000000004200770100000030420 08F0700000024306
33234663932612D363538612D343634612D383936342D303936616365613032636438000000000
```

4

Destroy (template)

In: uuidTemplate

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 80a5be03-1d2b-4190-917e-
34ed82a661b8
```

```
42007301000000904200720100000038420065010000002042006602000000040000000000000000042006702000000040
00000620000000042000D020000000400000001000000004200 0F0100000048420057050000000400000014000000004 2
00740100000003042008F0700000024383061356265303 32D316432622D343139302D393137652D3334656438326136363
1623800000000
```

Out: uuidTemplate

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8EB (Thu Jul 30
17:14:51 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
```

Deleted: 28 April

	Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 80a5be03-1d2b-4190-917e-34ed82a661b8 42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000000400000062000000042008E090000000800000004A71B8EB42000D020000000400000001000000004200F010000005842005705000000040000001400000000420070500000004000000000000000042007701000000304200F0700000024383061356265303 32D316432622D343139302D393137652D333465643832613636316238000000000

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

This use-case test 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.

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Normal, No bullets or numbering

Formatted: Font: 10 pt, Font color: Auto

Time	Request/Response messages
0	Create (symmetric key) In: objectType = '00000002', attributes={ Name={ NameValue='Key1', NameType='00000001' }, CryptographicAlgorithm='DES', CryptographicLength='56', CryptographicUsageMask='0000000C', ContactInformation='Joe' } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x42008D), 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 (0x420050), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x42004F), 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:

Deleted: 00000012'

Deleted: 28 April

```
          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


42007301000001984200720100000038420065010000002042006602000000040000000000000000420067020000000400
00000620000000042000D020000000400000001000000042000F0100000150420057050000000400000001000000004200
74010000013842005205000000040000000200000000042008D0100000120420008010000003842000A07000000044E6
16D650000000042000B01000000204200500700000044B6579310000000042004F0500000040000000100000000420000
08010000003042000A0700000017437279707 46F6772617068696320416C676F726974686D0042000B050000000400000
00100000000420008010000003042000A0700000014437279707 46F6772617068696320 4C656E6774680000000042000B
02000000040000003800000000420008010000003042000A0700000018437279707 46F6772617068696320557361676526
04D61736B42000B020000000400000000C000000004200080100000003042000A0700000013436F6E7461637420496E666F
726D6174696F6E000000000042000B07000000034A6F650000000000
```

Out: objectType = ‘00000002’, uuidKey

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8EB (Thu Jul 30
17:14:51 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d515c861-779c-4449-a745-
e9e91f950249


42007601000000C042007501000000484200650100000020420066020000000400000000000000004200670200000004 0
00000620000000042008E090000000800000000 4A71B8EB42000D020000000400000001000000042000F010000006842
00570500000004000000010000000042007A05000000040000000000000000420077010000004042005205000000040000
00002000000042008F0700000024643531356338363 12D373739632D343434392D613734352D653965393166393530323
43900000000
```

1 Locate (symmetric key)

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

Deleted: Name={

Deleted: ‘00000002’

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
```

Deleted: 28 April

	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 (0x420050), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x42004F), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007301000000D042007201000000384200650100000020420066020000000400000000000000004200670200000004000000620000000042000D020000000400000001000000042000F0100000088420057050000000400000008000000004200740100000070420008010000002842000A070000000B4F626A65637420547970650000000000042000B0500000004000000020000000042000801000000384200A070000000044E616D650000000042000B0100000020420050070000000044B657931000000042004F0500000004000000100000000 Out: uuidKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8EC (Thu Jul 30 17:14:52 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d515c861-779c-4449-a745-e9e91f950249 42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000000A71B8EC42000D020000000400000001000000004200F010000005842005705000000040000000800000000042007A050000000400000000000000004200770100000030420008F0700000024643531356338363132D373739632D343434392D613734352D653965393166393530323439000000000
2	Get (symmetric key) In: uuidKey Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d515c861-779c-4449-a745-

Deleted: 28 April

	e9e91f950249 42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000000042000D0200000004000000010000000042000F01000000484200570500000004000000000A00000000420074010000003042008F070000002464353135633836312D373739632D343434392D613734352D653965393166393530322343900000000 Out: objectType = ‘00000002’, uuidKey, symmetricKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8EC (Thu Jul 30 17:14:52 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d515c861-779c-4449-a745-e9e91f950249 Tag: Symmetric Key (0x42008A), Type: Structure (0x01), Data: Tag: Key Block (0x42003C), Type: Structure (0x01), Data: Tag: Key Value Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x42003F), Type: Structure (0x01), Data: Tag: Key Material (0x42003D), Type: Octet String (0x08), Data: 5BEAC8405BA41015 Tag: Cryptographic Algorithm (0x420025), Type: Enumeration (0x05), Data: 0x00000001 (DES) Tag: Cryptographic Length (0x420026), Type: Integer (0x02), Data: 0x00000038 (56) 420076010000011842007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000000004A71B8EC42000D0200000004000000010000000042000F01000000C04200570500000004000000000A0000000042007A0500000004000000000000000042007701000000984200520500000004000000020000000042008F070000002464353135633836312D373739632D343434392D613734352D653965393166393530323439000000000042008A010000005042003C0100000048420040050000000400000001000000042003F0100000010420003D08000000085BEAC8405BA410154200250500000004000000010000000042002602000000040000003800000000
3	Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420074), Type: Structure (0x01), Data:

Deleted: 28 April

	Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d515c861-779c-4449-a745-e9e91f950249 42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000004200D020000000400000001000000004200F0100000048420057050000000400000014000000004200740100000030420008F0700000024643531356338363 12D373739632D343434392D613734352D6539653931663935303 2343900000000 Out: uuidKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8EC (Thu Jul 30 17:14:52 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d515c861-779c-4449-a745-e9e91f950249 42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000004A71B8EC42000D020000000400000001000000004200F010000005842005705000000040000001400000000420078A050000000400000000000000004200770100000030420008F0700000024643531356338363 12D373739632D343434392D613734352D6539653931663935303 2343900000000
4	Locate In: uuidKey Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420074), 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: d515c861-779c-4449-a745-e9e91f950249 42007301000000B842007201000000384200650100000020420066020000000400000000000000004200670200000004000000620000000042000D020000000400000001000000004200F0100000070420057050000000400000008000000004200740100000058420008010000005042000A0700000011556E697175652049646 56E7469666965720000000000000042000B07000000246435313563383631 2D373739632D343434392D613734352D6539653931663935303 2343900000000	

Deleted: 28 April

	Out: <empty response payload>
	
	Tag: Response Message (0x420076), Type: Structure (0x01), Data:
	  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
	  Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8EC (Thu Jul 30 17:14:52 CEST 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
	  Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x420077), Type: Structure (0x01), Data: null
	
	420076010000008042007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000004A71B8EC42000D020000000400000001000000004200 0F010000002842005705000000040000000800000000042007A05000000040000000000000000420077010000000

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

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

This use-case demonstrates the fact that two clients may 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 a 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 would need to employ another policy than the Default policy defined in the KMIP specification on the key object to allow both clients to access it.

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Normal, No bullets or numbering

Formatted: Font color: Auto

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 (0x420073), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)

Deleted: templateName = 'Template1',

Deleted:

Deleted: ¶

Deleted:

Deleted: 28 April

```
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000003 (Register)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000006 (Template)
      Tag: Template-Attribute (0x42008D), 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 (0x420050), Type: Text String (0x07), Data: Template1
            Tag: Name Type (0x42004F), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)


420073010000013042007201000000384200650100000020420066020000000400000000000000004200670200000004000000620000000042000D020000000400000001000000004200F01000000E84200570500000004000000030000000042007401000000D042005205000000040000000600000000042008D01000000B84200080100000030420000A0700000017437279707467726170686963204164676F726974686D0042000B0500000004000000030000000042000801000000304200A0700000014437279707467726170686963204C656E6774680000000042000B020000000400000080000000004200080100000042042000A07000000044E616D650000000042000B0100000028420050070000000954656D706C6174656C617465310000000000000042004F0500000004000000010000000
```

Out: objectType='00000007', uuidTemplate

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8ED (Thu Jul 30
17:14:53 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000003 (Register)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000006 (Template)
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 08f9f9a2-3691-40b6-baa9-
dc6a116c74bb


42007601000000C042007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000004A71B8ED42000D020000000400000001000000004200F010000006842005705000000040000000300000000042007A05000000040000000000000004200770100000040420052050000000400000620000000042008F0700000024303866396639613322D333639312D343062362D626161392D6463366131313663373462620000000
```

1	Client A: Create (symmetric key using template)

Deleted: 28 April

In: objectType='00000002', template={ NameValue= 'Template1', NameType='00000001' }, attributes={ Name={ Name='Key1', NameType='00000001' }, CryptographicUsageMask='00000004', ContactInformation='Foo' }

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x42008D), Type: Structure (0x01), Data:
        Tag: Name (0x42004E), Type: Structure (0x01), Data:
          Tag: Name Value (0x420050), Type: Text String (0x07), Data: Template1
          Tag: Name Type (0x42004F), 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 (0x420050), Type: Text String (0x07), Data: Key1
            Tag: Name Type (0x42004F), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Foo
```

```
42007301000001584200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000042000D020000000400000001000000042000F0100000110420057050000000400000001000000004200740100000F842005205000000040000000200000000042008D01000000E042004E0100000028420050070000000954656D706C6174653100000000000000042004F0500000004000000010000000042000801000000384200A07000000044E616D650000000042000B0100000020420050070000000044B6579310000000042004F0500000004000000010000000042000801000000384200A07000000018437279707 46F6772617068696320557361676520 4D61736B42000B020000000400000004000000042000801000000384200A0700000013436F6E7461637420496E666F726D6174696F6E000000000042000B0700000003466F6F0000000000
```

Out: objectType='00000002', uuidKey

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8ED (Thu Jul 30
17:14:53 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
```

Deleted:

Deleted: 28 April

	Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-2d6fa4d2311e 42007601000000C042007501000000484200650100000020420066020000000400000000000000000420067020000000400000062000000000420 08E090000000800000000 4A71B8ED42000D020000000400000001000000004200 0F010000006842005705000000040000000100000000420 07A050000000400000000000000000420077010000004042005205000000040000002000000042008F070000002464313065333564372D383632662D343765342D396438652D32643666613464323331316500000000
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 (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: D5D4DD19F80FA0B5 Tag: Request Payload (0x420074), 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 (0x420050), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x42004F), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 0A477D6656E29BBA Tag: Request Payload (0x420074), Type: Structure (0x01), Data: null 42007301000001204200720100000048420065010000002042006602000000040000000000000000042006702000000040000006200000000042001006000000008000000000000000142000D020000000400000002000000004200 0F010000009842005705000000040000000800000000420090080000000 8D5D4DD19F80FA0B5420074010000007042000801000000284200A070000000B4F626A65637420547970650000000000042000B050000000400000002000000004200080100000038420000A07000000044E616D650000000042000B0100000020420050070000000044B65793100000000042004F0500000004000000100000000420 0F0100000028420057050000000040000000A0000000042009008000000080A477D6656E29BBA4200740100000000

Deleted: 28 April

	Out: uuidKey
	Out: objectType='00000002', uuidKey, symmetricKey
	
	Tag: Response Message (0x420076), Type: Structure (0x01), Data:
	  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
	  Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8EE (Thu Jul 30 17:14:54 CEST 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
	  Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: D5D4DD19F80FA0B5
	  Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-2d6fa4d2311e
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get)
	  Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 0A477D6656E29BBA
	  Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
	  Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
	  Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-2d6fa4d2311e
	  Tag: Symmetric Key (0x42008A), Type: Structure (0x01), Data:
	  Tag: Key Block (0x42003C), Type: Structure (0x01), Data:
	  Tag: Key Value Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001
	  Tag: Key Value (0x42003F), Type: Structure (0x01), Data:
	  Tag: Key Material (0x42003D), Type: Octet String (0x08), Data: 4BA2FB14F176929D3D2E7FA20F604B49
	  Tag: Cryptographic Algorithm (0x420025), Type: Enumeration (0x05), Data: 0x00000003 (AES)
	  Tag: Cryptographic Length (0x420026), Type: Integer (0x02), Data: 0x00000080 (128)
	
	42007601000001A042007501000000484200650100000020420066020000000400000000000000004200670200000004000000062000000004200 8E090000000800000004A71B8EE42000D020000000400000002000000004200 0F010000006842005705000000040000000800000000420090080000000 8D5D4DD19F80FA0B542007A05000000040000000000000000420077010000003042008F0700000024643130653335643 72D383632662D343765342D396438652D326436666134643233313165000000004200 8A01000005842003C0100000504200400500000004000000010000000042003F010000001842003D08000000104BA2FB14F176929D3D2E7FA20F604B4942002505000000040000000300000000420026020000000400000080000000

3	Client B: Get attribute list In: uuidKey Tag: Request Message (0x420073), Type: Structure (0x01), Data:

Deleted: 28 April

```
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-
2d6fa4d2311e
```

```
420073010000009042007201000000384200650100000020420066020000000400000000000000000420067020000000400
000006200000000420000D020000000400000001000000042000F0100000048420057050000000400000000C0000000042
007401000000303420008F0700000024643130653335643723D383632662D343765342D396438652D3264366661346432333
1316500000000
```

Out: uuidKey, attributes={ * }

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8EE (Thu Jul 30
17:14:54 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-
2d6fa4d2311e
      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
```

```
42007601000001D042007501000000484200650100000020420066020000000400000000000000000420067020000000400
000006200000000420008E090000000800000000A71B8EE42000D020000000400000001000000000420000F010000017842
005705000000040000000C0000000042007A050000000400000000000000000420077010000015042008F0700000024643
13065333564372D383632662D343765342D396438652D3264366661346432333131650000000042000A07000000144372
7970746F67726170686963204C656E6774680000000042000A0700000017437279707 46F67726170686963204 16C676F7
26974686D0042000A0700000005537461746500000042000A0700000006446967657374000042000A070000000C496E69
7469616C204461746500000000042000A0700000011556E6971756520496 4656E74696669657200000000000000042000A0
7000000044E616D650000000042000A0700000018437279707 46F67726170686963205573616765204D61736B42000A07
0000000B4F626A6563742054797065000000000042000A0700000013436F6E7461637420496E666F726D6174696F6E000
```

Deleted: 28 April

	000000042000A07000000114C617374204368616E67656420446174650000000000000
4	Client B: Get attributes In: uuidKey, attributeNames={'Name', 'ContactInformation'} Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-2d6fa4d2311e Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information 42007301000000C042007201000000384200650100000020420066020000000400000000000000004200670200000004000000620000000042000D020000000400000001000000042000F0100000078420057050000000400000000B000000004200740100000006042008F0700000024643130653335645372D383632662D343765342D396438652D3264366661346432331316500000000042000A07000000044E616D6500000000042000A0700000013436F6E7461637420496E666F726D6174696F6E0000000000 Out: uuidKey, attributes={ Name={ Name='Key1', NameType='00000001' }, ContactInformation='Foo' } Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8EE (Thu Jul 30 17:14:54 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-2d6fa4d2311e 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 (0x420050), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x42004F), 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

Deleted: 28 April

	42007601000001284200750100000048420065010000002042006602000000040000000000000000420067020000000400000062000000004200 8E090000000800000000 4A71B8EE42000D020000000400000001000000004200 0F01000000D042005705000000004000000 0B00000000420070A050000000400000000000000004200770100000 0A842008F0700000024643130653335643720D383632662D343765342D396438652D326436666134643233313165000000004200080100000038420000A07000000044E616D650000000042000B0100000020420050070000000044B65793100000000420040F050000000400000010000000042000801000000 3042000A0700000013436F6E7461637420496E666F726D6174696F6E000000000042000B0700000003466F6F0000000000
5	Client B: Add attribute [batch] In: uuidKey, attribute={ x-attribute1='Value1'} In: uuidKey, attribute={ x-attribute2='Value2' } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 58E94E8970FFB88B Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-2d6fa4d2311e 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 8AD0A151238C7B7C Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-2d6fa4d2311e 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 42007301000001604200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000004200 0D020000000400000002000000004200 0F01000000884200570500000000400000000D0000000042009008000000085 8E94E8970FFB88B4200740100000006042008F0700000024643130653335643720D383632662D343765342D396438652D326436666134643233313165000000004200801000000284200 0A070000000C782D6174747269627574653100000000420008B0700000006566 16C7565310000420000F0100000088420057050000000040000000D0000000042008000000088AD0A151238C7B7C4200740100000006042008F0700000024643130653335643720D383632662D343765342D396438652D326436666134643233313165000000004200801000000284200 0A070000000C782D6174747269627574653200000000420008B0700000006566 16C7565320000 Out: uuidKey, attribute={ x-attribute1='Value1'} Out: uuidKey, attribute={ x-attribute2='Value2' } Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data:

Deleted: 28 April

```
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8EE (Thu Jul 30
17:14:54 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 58E94E8970FFB88B
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-
2d6fa4d2311e
      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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 8AD0A151238C7B7C
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-
2d6fa4d2311e
      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


42007601000001904200750100000048420065010000002042006602000000040000000000000000420067020000000400
00000620000000042008E090000000800000004A71B8EE42000D020000000400000002000000004200 0F010000009842
00570500000004000000D0000000042009008000000858E94E8970FFB88B42007A050000000400000000000000000420
07701000000604200 8F07000000246431306533356437 2D383632662D343765342D396438652D32643666613464323331
31650000000042000801000000 2842000A070000000C782D6174747269627574653100000000042000B070000000656616
C756531000042000F0100000098420057050000000400000000D0000000042009008000000088AD0A151238C7B7C42007A
05000000040000000000000000042007701000000604200 8F07000000246431306533356437 2D383632662D343765342D3
96438652D32643666613464323331316500000000420008010000002842000A070000000C782D6174747269627574653 2
0000000042000B070000000656616C7565320000
```

6 Client B:

Modify attribute [batch]

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

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

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 361C8B13C749A31F
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-
```

Deleted: 28 April

```
2d6fa4d2311e
      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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 0BD5758C795439AE
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-
2d6fa4d2311e
      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


420073010000017042007201000000384200650100000020420066020000000400000000000000004200670200000004000006200000000042000D020000000400000002000000004200 0F0100000090420057050000000400000000E0000000042009008000000008361C8B13C749A31F4200740100000068420 08F07000000246431306533356437 2D383632662D343765342D396438652D326436666134643233313165000000004200080100000030420 0A070000000C782D6174747269627574653100000000042000B070000000E4D6F6469666965645661 6C756531000042000F0100000090420057050000000400000000E000000004200900800000000 80BD5758C795439AE4200740100000068420 08F07000000246431306533356437 2D383632662D343765342D396438652D326436666134643233313165000000004200080100000030420 0A070000000C782D6174747269627574653200000000042000B070000000E4D6F6469666965645661 6C7565320000
```

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

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

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8EF (Thu Jul 30
17:14:55 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 361C8B13C749A31F
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-
2d6fa4d2311e
      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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 0BD5758C795439AE
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-
2d6fa4d2311e
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
```

Deleted: 28 April

	Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2 42007601000001A042007501000000484200650100000020420066020000000400000000000000000420067020000000400000062000000004200 8E090000000800000000 4A71B8EF42000D020000000400000002000000004200 0F01000000A042005705000000040000000E000000004200900800000008361C8B13C749A31F42007A0500000004000000000000000042007701000000684200 8F0700000024643130653335643720D383632662D343765342D396438652D326436666134643233313165000000004200 80100000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F64696696564566 16C756531000042000F01000000A042005705000000004000000E000000004200900800000008 0BD5758C795439AE42007A0500000004000000000000000042007701000000684200 8F0700000024643130653335643720D383632662D343765342D396438652D326436666134643233313165000000004200 0A070000000C782D617474726962757465320000000042000B070000000E4D6F64696696564566 16C7565320000
7	Client B: Delete attribute [batch] In: uuidKey, attributeNames={'x-attribute1'} In: uuidKey, attributeNames={'x-attribute2'} Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute) Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 71FE1FBB074EFE2F Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-2d6fa4d2311e Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute) Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 5F5B437A980D0306 Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-2d6fa4d2311e Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 42007301000001304200720100000038420065010000002042006602000000040000000000000000042006702000000040000006200000000420 0D020000000400000002000000004200 0F01000000704200570500000004000000 0F0000000042009008000000085F5B437A980D0306420074010000004842008F07000000246431306533356437 2D383632662D343765342D396438652D326436666134643233313165000000004200 0A070000000C782D617474726962757465320000000000 Out: uuidKey, attributeNames={'x-attribute1'} Out: uuidKey, attributeNames={'x-attribute2'} Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:

Deleted: 28 April

	Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8EF (Thu Jul 30 17:14:55 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute) Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 71FE1FBB074EFE2F Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-2d6fa4d2311e 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute) Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 5F5B437A980D0306 Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-2d6fa4d2311e 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 42007601000001A042007501000000484200650100000020420066020000000400000000000000000420067020000000400000062000000004200 8E090000000800000000 4A71B8EF42000D020000000400000002000000004200 0F01000000A04200570500000004000000000000000042007701000000684200 8F07000000246431306533356437 2D383632662D343765342D396438652D32643666613464323331316500000000420008010000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F6469666965645661 6C756531000042000F01000000A042005705000000040000000F000000004200900800000000871FE1FBB074EFE2F42007A05000000040000000000000000420077010000006842008F07000000246431306533356437 2D383632662D343765342D396438652D326436666134643233313165000000004200080100000030420 00A070000000C782D6174747269627574653100000000420 00B070000000E4D6F6469666965645661 6C7565320000042000B070000000E4D6F6469666965645661 6C7565320000
8	Client A: Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-2d6fa4d2311e 42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400000090420072010000003842006501000000204200660200000004000000000000000042006702000000040

Deleted: 28 April

	0000062000000042000D020000000400000001000000042000F0100000048420057050000000400000014000000004200740100000003042008F0700000024643130653335643 72D383632662D343765342D396438652D3264366661346432333 1316500000000 Out: uuidKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F0 (Thu Jul 30 17:14:56 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-2d6fa4d2311e 42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000004000000062000000042008E090000000800000004A71B8F042000D020000000400000001000000042000F010000005842005705000000040000001400000000042007A050000000400000000000000004200770100000003042008F0700000024643130653335643 72D383632662D343765342D396438652D3264366661346432333131650000000
9	Client A: Get (symmetric key) In: uuidKey Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: d10e35d7-862f-47e4-9d8e-2d6fa4d2311e 42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400000006200000000420 00D020000000400000001000000042000F0100000048420057050000000400000000A00000000420074010000003042008F0700000024643130653335643 72D383632662D343765342D396438652D3264366661346432333 1316500000000 Out: Operation Failed, Item Not Found Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data:

Deleted: 28 April

	Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F0 (Thu Jul 30 17:14:56 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000001 (Failed) Tag: Result Reason (0x420079), Type: Enumeration (0x05), Data: 0x00000001 (Item Not Found) Tag: Result Message (0x420078), Type: Text String (0x07), Data: No Cryptographic Object found with given Unique Identifier 42007601000000D042007501000000484200650100000020420066020000000400000000000000004200670200000004000000062000000004200 8E090000000800000004A71B8F042000D020000000400000001000000004200 0F010000007842005705000000040000000A0000000042007A0500000004000000010000000042007905000000040000001000000004200780700000003A4E6F2043727970746F6772617068696320 4F626A65637420666F756E64207769746820676976656E20556E697175652049646564E7469666965720000000000000
10	Client A: Destroy (template) In: uuidTemplate Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 08f9f9a2-3691-40b6-baa9-dc6a116c74bb 42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400000006200000000420 0D020000000400000001000000004200 0F01000000484200570500000004000000140000000042007401000000304200 8F0700000024303866396639613 22D333639312D343062362D626161392D6463366131313663734626200000000 Out: uuidTemplate Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F0 (Thu Jul 30 17:14:56 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

Deleted: 28 April

	Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 08f9f9a2-3691-40b6-baa9-dc6a116c74bb 42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000004000000062000000004200 8E090000000800000004A71B8F042000D020000000400000001000000004200 0F010000005842005705000000040000001400000000420 07A050000000400000000000000004200770100000030420 08F0700000024303866396639613220D333639312D343062362D626161392D6463366131313663373462620000000
11	Client A: Get (template) In: uuidTemplate Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 08f9f9a2-3691-40b6-baa9-dc6a116c74bb 42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400000006200000000420 0D020000000400000001000000004200 0F010000048420057050000000400000 0A000000004200740100000030420 08F070000002430386639663961322D333639312D343062362D626161392D6463366131313663373462620000000 Out: Operation Failed, Item Not Found Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F0 (Thu Jul 30 17:14:56 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000001 (Failed) Tag: Result Reason (0x420079), Type: Enumeration (0x05), Data: 0x00000001 (Item Not Found) Tag: Result Message (0x420078), Type: Text String (0x07), Data: No Cryptographic Object found with given Unique Identifier 42007601000000D042007501000000484200650100000020420066020000000400000000000000004200670200000004000000062000000004200 8E090000000800000004A71B8F042000D020000000400000001000000004200 0F010000007842005705000000040000000A0000000042007 A05000000040000000100000000420079050000000400000001000000004200780700000003A4E6F2043727970746F67726170686963204F626A65637420666F756E642077697468206769766 56E2055 6E6971756520496465 6E74696669657200000000000

Deleted: 28 April

3.2 Use-case: Asynchronous Locate

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

This use-case shows the use of two clients with the same assumptions as in the use-case described in Section 3.1.4 Since the client cannot force the server to respond asynchronously, a server may respond synchronously to the requests issued at times 1 and 4, in which case the expected response will be the ones shown at times 2 and 5, respectively. In the case of the server not responding asynchronously to the Locate requests, the requests illustrated at time 7 and 8 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' }
	
	`Tag: Request Message (0x420073), Type: Structure (0x01), Data:`
	`  Tag: Request Header (0x420072), Type: Structure (0x01), Data:`
	`  Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:`
	`  Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)`
	`  Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Create)`
	`  Tag: Request Payload (0x420074), Type: Structure (0x01), Data:`
	`  Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)`
	`  Tag: Template-Attribute (0x42008D), 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 (0x420050), Type: Text String (0x07), Data: Key1`
	`  Tag: Name Type (0x42004F), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)`
	`  Tag: Attribute (0x420008), Type: Structure (0x01), Data:`

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Deleted: I

Formatted: Indent: First line: 0 pt

Formatted: Indent: First line: 0 pt, Don't adjust space between Latin and Asian text

Deleted: 1

Deleted: , ObjectGroup='Group1'

Deleted: ¶ CryptographicAlgorithm='AES', ¶ CryptographicLength='128',

Deleted: 28 April

```
          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


42007301000001904200720100000038420065010000002042006602000000040000000000000000420067020000000400
00000620000000042000D020000000400000001000000004200 0F0100000148420057050000000400000001000000004200
74010000013042005205000000040000000200000000420 08D0100000118420008010000003042000A0700000017437
27970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200
0A0700000014437279707 46F6772617068696320 4C656E6774680000000042000B020000000400000080000000004200
80100000038420 00A07000000044E616D650000000042000B0100000020420050070000000044B6579310000000042004F
0500000004000000010000000042000801000000304200 0A07000001843727970746F6772617068696320557361676520
04D61736B42000B020000000400000004000000004200080100000028420 00A070000000C4F626A6563742047726F7570
0000000042000B070000000647726F7570310000
```

Out: objectType = ‘00000002’, uuidKey

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F1 (Thu Jul 30
17:14:57 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 2f45993b-9af6-4b75-a990-
d6211814ea11


42007601000000C042007501000000484200650100000020420066020000000400000000000000004200670200000004 00
00000620000000042008E090000000800000004A71B8F142000D020000000400000001000000004200 0F010000006842
00570500000004000000010000000042007A05000000040000000000000004200770100000040420052050000000400 0
00020000000042008F0700000024326634353939336 22D396166362D346237352D613939302D643632313138313465 61
313100000000
```

1 Client B:

Locate (symmetric key by name)

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

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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)
```

Deleted: 2

Deleted: 28 April

```
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420074), 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 (0x420050), Type: Text String (0x07), Data: Key1
          Tag: Name Type (0x42004F), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)


42007301000000E042007201000000484200650100000020420066020000000400000000000000004200670200000004000
0000062000000004200070600000008000000000000000142000D020000000400000001000000004200 0F010000008842
00570500000004000000080000000042007401000000704200080100000028420 00A070000000B4F626A6563742054797
0650000000000042000B0500000004000000020000000042000801000000 3842000A07000000044E616D650000000042000
0B0100000020420050070000000044B65793100000000042004F0500000004000000010000000 0
```

Out: asyncCorrValue1

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F1 (Thu Jul 30
17:14:57 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000002 (Pending)
    Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:
40736460C5C6EEBD


42007601000000884200750100000048420065010000002042006602000000040000000000000000420067020000000400
0000062000000004200 8E090000000800000000 4A71B8F142000D020000000400000001000000004200 0F010000003042
00570500000004000000080000000042007A0500000004000000020000000042000608000000 0840736460C5C6EEBD
```

2 Client B:

Poll*

In: asyncCorrValue1

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000001A (Poll)
```

Deleted: 3

Deleted: 28 April

```
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:
40736460C5C6EEBD


42007301000000704200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000004200D020000000400000001000000004200F0100000028420057050000000400000001A0000000042007401000000104200608000000840736460C5C6EEBD
```

Out: uuidKey1

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F1 (Thu Jul 30
17:14:57 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 2f45993b-9af6-4b75-a990-
d6211814ea11


42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000000A71B8F142000D020000000400000001000000004200F010000005842005705000000040000000800000000042007A05000000040000000000000000420077010000003042008F0700000024326634353939336 22D396166362D346237352D613939302D6436323131383134656131310000000
```

3 Client B:

Get (symmetric key)

In: uuidKey1

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 2f45993b-9af6-4b75-a990-
d6211814ea11


42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000004200D020000000400000001000000004200F0100000048420057050000000400000000A0000000042007401000000304200 8F07000000243266343539393362 2D396166362D346237352D613939302D6436323131383134656 1313100000000
```

Out: objectType = ‘00000002’, uuidKey1, symmetricKey

Deleted: 4

Deleted: 28 April

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F1 (Thu Jul 30
17:14:57 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 2f45993b-9af6-4b75-a990-
d6211814ea11
      Tag: Symmetric Key (0x42008A), Type: Structure (0x01), Data:
        Tag: Key Block (0x42003C), Type: Structure (0x01), Data:
          Tag: Key Value Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x42003F), Type: Structure (0x01), Data:
            Tag: Key Material (0x42003D), Type: Octet String (0x08), Data:
C3F5135717E01CBB7DD476CB70AC47A6
          Tag: Cryptographic Algorithm (0x420025), Type: Enumeration (0x05), Data: 0x00000003
(AES)
          Tag: Cryptographic Length (0x420026), Type: Integer (0x02), Data: 0x00000080 (128)


42007601000001204200750100000048420065010000002042006602000000040000000000000000420067020000000400000062000000042008E090000000800000004A71B8F142000D020000000400000001000000004200F01000000C84200570500000004000000A00000000420070A0500000004000000000000000042007701000000A042005205000000040000000042008F070000002432663435393933622D396166362D346237352D613939302D643632313138313465613131000000042008A01000000584200 3C0100000050420040050000000400000001000000004200 3F010000001842003D0800000010C3F5135717E01CBB7DD476CB70AC47A64200250500000004000000030000000042002602000000040000008000000000
```

4 Client B:

Locate (symmetric key by group)

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

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420074), 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)
```

Deleted: 5

Deleted: 28 April

```
      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


42007301000000D042007201000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042000706000000008000000000000000142000D020000000400000001000000004200F010000007842005705000000040000000800000000420074010000006042000801000000284200A070000000B4F626A6563742054797065000000000042000B050000000400000002000000004200080100000028420 00A070000000C4F626A6563742047726F757000000000042000B07000000647726F7570310000
```

Out: asyncCorrValue2

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F1 (Thu Jul 30 17:14:57 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000002 (Pending)
    Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 140C3B936914BEE5


42007601000000884200750100000048420065010000002042006602000000040000000000000000420067020000000400000062000000004200 8E090000000800000004A71B8F142000D020000000400000001000000004200F010000003042005705000000040000000800000000420 07A050000000400000002000000004200608000000008140C3B936914BEE5
```

5 Client B:

Poll*

In: asyncCorrValue2

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000001A (Poll)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 140C3B936914BEE5


42007301000000704200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000004200D020000000400000001000000004200F0100000028420057050000000400000001A0000000420074010000001042000608000000008140C3B936914BEE5
```

Out: uuidKey2

Deleted: 6

Deleted: 28 April

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F1 (Thu Jul 30
17:14:57 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 2f45993b-9af6-4b75-a990-
d6211814ea11


42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000004
0000006200000000042008E090000000800000004A71B8F142000D020000000400000001000000004200 0F010000005842
00570500000004000000080000000042007A05000000040000000000000004200770100000030420 08F0700000024326
63435393933622D396166362D346237352D613939302D643632313138313465613131 00000000
```

6 Client B:

Get (symmetric key)

In: uuidKey2

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 2f45993b-9af6-4b75-a990-
d6211814ea11


42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400
0000062000000004200 0D020000004000000010000000042000F0100000048420057050000000400000000A0000000042
00740100000030420 08F0700000024326634353939336 22D396166362D346237352D613939302D643632313138313465 6
1313100000000
```

Out: objectType = ‘00000002’, uuidKey2, symmetricKey

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F2 (Thu Jul 30
17:14:58 CEST 2009)
```

Deleted: 7

Deleted: 28 April

```
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 2f45993b-9af6-4b75-a990-
d6211814ea11
      Tag: Symmetric Key (0x42008A), Type: Structure (0x01), Data:
        Tag: Key Block (0x42003C), Type: Structure (0x01), Data:
          Tag: Key Value Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x42003F), Type: Structure (0x01), Data:
            Tag: Key Material (0x42003D), Type: Octet String (0x08), Data:
C3F5135717E01CBB7DD476CB70AC47A6
          Tag: Cryptographic Algorithm (0x420025), Type: Enumeration (0x05), Data: 0x00000003
(AES)
          Tag: Cryptographic Length (0x420026), Type: Integer (0x02), Data: 0x00000080 (128)


42007601000001204200750100000048420065010000002042006602000000040000000000000000042006702000000040
0000062000000042008E090000000800000004A71B8F242000D020000000400000001000000042000F01000000C842
00570500000004000000A0000000042007A0500000004000000000000000042007701000000A042005205000000040000
0000200000000042008F070000002432663435393933622D396166362D346237352D613939302D643632313138313461
3131000000042008A010000005842003C010000005042004005000000040000000100000000042003F010000001842003
D0800000010C3F5135717E01CBB7DD476CB70AC47A64200250500000004000000030000000042002602000000040000000
8000000000
```

7 Client B:

Locate (symmetric key by name)

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

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420074), 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 (0x420050), Type: Text String (0x07), Data: Key1
          Tag: Name Type (0x42004F), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)


42007301000000E042007201000000484200650100000020420066020000000400000000000000004200670200000004 0
```

Deleted: 8

Deleted: 28 April

```
0000062000000004200070600000008000000000000000142000D020000000400000001000000004200F010000008842
00570500000004000000080000000042007401000000704200080100000028420000A070000000B4F626A6563742054797
0650000000000042000B0500000004000000020000000042000801000000384200A07000000044E616D65000000004200
0B0100000020420050070000000044B65793100000000042004F0500000004000000100000000
```

Out: asyncCorrValue5

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F2 (Thu Jul 30
17:14:58 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000002 (Pending)
    Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:
F6E77C5F2C1B74E0
```

```
420076010000008842007501000000484200650100000020420066020000000400000000000000004200670200000004 0
0000062000000004200 8E090000000800000004A71B8F242000D020000000400000001000000004200 0F010000003042
00570500000004000000080000000042007A0500000004000000020000000042000608000000008F6E77C5F2C1B74E0
```

8 Client B:

Cancel

In: asyncCorrValue5

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000019 (Cancel)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:
F6E77C5F2C1B74E0
```

```
420073010000007042007201000000384200650100000020420066020000000400000000000000004200670200000004 0
0000062000000004200 D020000000400000001000000004200 0F0100000028420057050000000400000019000000004 2
00740100000010420006080000000 8F6E77C5F2C1B74E0
```

Out: asyncCorrValue5, CancelResult='00000001'

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
```

Deleted: 9

Deleted: 28 April

```
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F2 (Thu Jul 30
17:14:58 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000019 (Cancel)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:
F6E77C5F2C1B74E0
      Tag: Cancellation Result (0x420012), Type: Enumeration (0x05), Data: 0x00000001 (Cancelled)


42007601000000A042007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000004A71B8F242000D020000000400000001000000004200
0F010000004842005705000000040000001900000000420007A050000000400000000000000004200770100000020420006080000000
8F6E77C5F2C1B74E042001205000000040000000100000000
```

9

Client A:

Destroy (symmetric key)

In: uuidKey

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 2f45993b-9af6-4b75-a990-
d6211814ea11


42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000004200
0D020000000400000001000000004200F0100000048420057050000000400000014000000004200740100000030420
08F07000000243266343539393362
2D396166362D346237352D613939302D643632313138313465613131310000000
```

Out: uuidKey

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F2 (Thu Jul 30
17:14:58 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
```

Deleted: 10

Deleted: 28 April

	Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 2f45993b-9af6-4b75-a990-d6211814ea11 42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000000400000062000000004200 8E090000000800000004A71B8F242000D020000000400000001000000004200 0F010000005842005705000000040000001400000000042007A0500000004000000000000000004200770100000030420 08F0700000024326634353939336 22D396166362D346237352D613939302D6436323131383134656131310000000 0

* = 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 may or may not do with the key). To clean up, the created key is finally destroyed..

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Deleted: ¶

Formatted: Indent: First line: 0 pt

Time	Client A
0	Client A: Create (symmetric key) In: objectType = '00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', Name={ NameValue='Key1', NameType='00000001' }, CryptographicUsageMask='00000004' }

Deleted: CryptographicAlgorithm='AES', ¶ CryptographicLength='128',

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x42008D), 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:
```

Deleted: 28 April

	Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420050), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x42004F), 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) 42007301000001604200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000004200D020000000400000001000000004200F0100000118420057050000000400000001000000004200741000001004200520500000004000000020000000042008D01000000E842000801000000342000A0700000017437279707467726170686963204167 6F726974686D0042000B0500000004000000030000000042000801000000304200 0A0700000014437279707467726170686963204C656E6774680000000042000B020000000400000080000000004200080100000038420 00A07000000044E616D650000000042000B0100000020420050070000000 44B6579310000000042004F050000000400000001000000004200801000000304200 0A07000000184372797074 6F772617068696320557361676520 4D61736B42000B020000000400000004000000 00 Out: objectType = ‘00000002’, uuidKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F2 (Thu Jul 30 17:14:58 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 42007601000000C042007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000000 4A71B8F242000D020000000400000001000000004200F010000006842005705000000040000000100000000420 07A0500000004000000000000000000420077010000004042005205000000040000000200000042008F0700000024323263626531343 32D666564622D343230392D386134332D6330366161396563386535360000000 0 Out: uuidKey, attributeName={‘State’}
1	Client A: Get attribute In: uuidKey, attributeName={‘State’} Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

Deleted: 28 April

	Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 42007301000000A042007201000000384200650100000020420066020000000400000000000000004200670200000004000000620000000042000D020000000400000001000000004200F0100000058420057050000000400000000B0000000042007401000000404200 8F07000000243232636265313433 2D666564622D343230392D386134332D633036616139656338653536000000004200801000000020420000A07000000055374617465000000 Out: uuidKey, attribute={ State='00000001' } Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F3 (Thu Jul 30 17:14:59 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 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) 42007601000000D842007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000000 4A71B8F342000D020000000400000001000000004200F010000008042005705000000040000000B0000000042007A05000000040000000000000000420077010000005842008F0700000024323236362653134332D666564622D343230392D386134332D633036616139656338653536000000004200801000000020420000A07000000055374617465000000042000B050000000400000001000000
2	Client A: Add attribute In: uuidKey, attribute={ ActivationDate='2' } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-

Deleted: 28 April

	c06aa9ec8e56 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) 42007301000000C042007201000000384200650100000020420066020000000400000000000000004200670200000004000000620000000042000D020000000400000001000000004200F0100000078420057050000000400000000D0000000042007401000000604200 8F07000000243232636265313433 2D666564622D343230392D386134332D633036616139656338653536000000004200801000000284200A070000000F41637469766174696F6E204461746500420 00B090000000800000000000002 Out: uuidKey, attribute={ ActivationDate='2' } Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F3 (Thu Jul 30 17:14:59 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 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) 42007601000000E042007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E09000000008000000004A71B8F342000D020000000400000001000000004200F010000008842005705000000040000000D0000000042007A05000000040000000000000000420077010000006042008F0700000024323 2636265313433 2D666564622D343230392D386134332D633036616139656338653536000000004200801000000284200A070000000F41637469766174696F6E204461746500420 00B090000000800000000000002
3	Client A: Get attribute In: uuidKey, attributeName={ 'State' } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420074), Type: Structure (0x01), Data:

Deleted: 28 April

	Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 42007301000000A042007201000000384200650100000020420066020000000400000000000000004200670200000004000000620000000042000D020000000400000001000000004200F0100000058420057050000000400000000B00000000420074010000004042008F0700000024323263626531343 32D666564622D343230392D386134332D633036616139656338653536000000004200801000000020420000A0700000005537461746500000042000A07000000055374617465000000 Out: uuidKey, attribute={ State='00000002' } Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F3 (Thu Jul 30 17:14:59 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active) 42007601000000D842007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000004A71B8F342000D020000000400000001000000004200F010000008042005705000000040000000B00000000420074A05000000040000000000000000420077010000005842008F0700000024323263626531343 32D666564622D343230392D386134332D633036616139656338653536000000004200801000000020420000A0700000005537461746500000042000B05000000040000000200000000
4	Client B: Locate (symmetric key by name) In: objectType = '00000002', attributes={ Name={ Name='Key1', NameType='00000001' } } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420074), 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)

Deleted: 28 April

	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 (0x420050), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x42004F), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007301000000D042007201000000384200650100000020420066020000000400000000000000004200670200000004000000620000000042000D020000000400000001000000004200F0100000088420057050000000400000008000000004200740100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000020000000042000801000000384200A070000000044E616D650000000042000B0100000020420050070000000044B65793100000000042004F0500000004000000010000000 Out: uuidKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F4 (Thu Jul 30 17:15:00 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000004A71B8F442000D020000000400000001000000004200F010000005842005705000000040000000800000000042007A05000000040000000000000000042007701000000304200 8F0700000024323 26362653134332D666564622D343230392D386134332D6330366161396563386535360000000
5	Client B: Get (symmetric key) In: uuidKey Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000040

Deleted: 28 April

	0000062000000042000D020000004000000010000000042000F0100000048420057050000000400000000A0000000042 00740100000003042008F0700000024323263626531343332D666564622D343230392D386134332D6330366161396563386 5353600000000 Out: objectType = '00000002', uuidKey, symmetricKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F5 (Thu Jul 30 17:15:01 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43- c06aa9ec8e56 Tag: Symmetric Key (0x42008A), Type: Structure (0x01), Data: Tag: Key Block (0x42003C), Type: Structure (0x01), Data: Tag: Key Value Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x42003F), Type: Structure (0x01), Data: Tag: Key Material (0x42003D), Type: Octet String (0x08), Data: 176CFFCB50904DB2AFD75D1FFF74F14F Tag: Cryptographic Algorithm (0x420025), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x420026), Type: Integer (0x02), Data: 0x00000080 (128) 42007601000001204200750100000048420065010000002042006602000000040000000000000000420067020000000400 0000062000000042008E0900000008000000004A71B8F542000D020000000400000001000000042000F01000000C842 00570500000004000000A0000000042007A0500000004000000000000000042007701000000A042005205000000040000 0000200000000042008F0700000024323263626531343332D666564622D343230392D386134332D6330366161396563386 5 3536000000042008A0100000058420030C0100000050420040050000000400000001000000042003F010000001842003 D0800000010176CFFCB50904DB2AFD75D1FFF74F14F4200250500000004000000030000000042002602000000040000000 8000000000
6	Client B: Revoke (symmetric key as compromised) In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceTime='6' Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000013 (Revoke) Tag: Request Payload (0x420074), Type: Structure (0x01), Data:

Deleted: 28 April

	Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 Tag: Revocation Reason (0x42007C), Type: Structure (0x01), Data: Tag: Revocation Reason Code (0x42007D), Type: Enumeration (0x05), Data: 0x00000001 (Key Compromise) Tag: Compromise Occurrence Date (0x42001E), Type: Date-Time (0x09), Data: 0x0000000000000006 (Thu Jan 01 01:00:06 CET 1970) 42007301000000B84200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000042000D020000000400000001000000042000F0100000070420057050000000400000013000000004200741000000584200 8F07000000243232636265313433 2D666564622D343230392D386134332D6330366161396563386535360000000042007C0100000010420 07D050000000400000001000000042001E090000000800000000000000006 Out: uuidKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F5 (Thu Jul 30 17:15:01 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000013 (Revoke) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000420 08E090000000800000000 4A71B8F542000D020000000400000001000000004200 0F010000005842005705000000040000001300000000420 07A050000000400000000000000004200770100000003042008F0700000024323 26362653134332D666564622D343230392D386134332D6330366161396563386535360000000
7	Client B: Get attribute In: uuidKey, attributeName={ ‘State’ } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

Deleted: 28 April

	42007301000000A042007201000000384200650100000020420066020000000400000000000000004200670200000004000000620000000042000D020000000400000001000000004200F0100000058420057050000000400000000B0000000042007401000000404200 8F07000000243232636265313433 2D666564622D343230392D386134332D633036616139656338653536000000004200801000000020420000A0700000005537461746500000042000B0500000004000000040000000
8	Client A: Get attribute list In: uuidKey

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-
c06aa9ec8e56
```

```
42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000004200 0D020000000400000001000000004200F0100000048420057050000000400000000C0000000042007401000000304200 8F07000000243232636265313433 2D666564622D343230392D386134332D633036616139656338653536000000005
```


Deleted: 28 April

	Out: uuidKey, attributes = { * } Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F5 (Thu Jul 30 17:15:01 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Compromise Occurrence Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Compromise Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digest Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Initial Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Revocation Reason Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Unique Identifier Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Last Changed Date 42007601000002284200750100000048420065010000002042006602000000040000000000000000420067020000000400000062000000004200 8E090000000800000004A71B8F542000D020000000400000001000000004200F01000001D042005705000000040000000C00000000420 07A05000000040000000000000000420077010000001A842008F0700000024323263626530 13433230392D386134332D633036616139656338653536000000004200 0A07000000144372797074 6F6772617068696320416C676F726974686D0042000A07000000055374617465000000042000A070000001A436F6D70726F6D697365204F6363757272656E6365204461746500000000000042000A070000000F436F6D70726F6D6973652044617465004200 0A07000000064469676573740000042000A070000000C496E697469616C20446174650000000042000A070000000F41637469766174696F6E2044617465004200 0A07000000115265766F636174696F6E20526561736F6E0000000000000042000A0700000011556E697175652049646564E7469666965720000000000000042000A07000000044E616D650000000042000A0700000184372797074 6F6772617068696320557361676520 4D61736B42000A070000000B4F626A656374205479706500000000042000A07000000114C617374204368616E676564204461746500000000000000
9	Client A: Get attributes In: uuidKey, attributeName = { ‘State’ } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)

Deleted: 28 April

	Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 42007301000000A042007201000000384200650100000020420066020000000400000000000000004200670200000004000000620000000042000D020000000400000001000000004200F0100000058420057050000000400000000B000000004200741000000042008F0700000024323263626531343320D666564622D343230392D386134332D6330366161396563386535360000000042000A07000000055374617465000000 Out: uuidKey, attribute={ State='00000004' } Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F5 (Thu Jul 30 17:15:01 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 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) 42007601000000D842007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000004A71B8F542000D020000000400000001000000004200F010000008042005705000000040000000B00000000420074A0500000004000000000000000042007701000000584200F0700000024323263626531343320D666564622D343230392D386134332D6330366161396563386535360000000042000801000000204200A0700000005537461746500000042000B0500000004000000040000000
10	Client A: Add attribute [batch] In: uuidKey, attribute={ x-attribute1='Value1' } In: uuidKey, attribute={ x-attribute2='Value2' } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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: 28 April

```
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 4B1F8ADA814C41DE
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-
c06aa9ec8e56
      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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 9E3FC11EE4C2767B
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-
c06aa9ec8e56
      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


42007301000001604200720100000038420065010000002042006602000000040000000000000000420067020000000400
0000062000000004200 0D020000000400000002000000004200 0F010000008842005705000000040000000D0000000042
009008000000084B1F8ADA814C41DE4200740100000060420 08F0700000024323263626531343 32D666564622D3432303
92D386134332D6330366161396563386535360000000042000801000000 2842000A070000000C782D6174747269627574
653100000000420 00B070000000656616C756531000042000F010000008842005705000000040000000D0000000042009
008000000089E3FC11EE4C2767B4200740100000060420 08F0700000024323263626531343 32D666564622D343230392D
386134332D6330366161396563386535360000000042000801000000 2842000A070000000C782D6174747269627574653
20000000420 00B070000000656616C7565320000
```

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

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

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F6 (Thu Jul 30
17:15:02 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 4B1F8ADA814C41DE
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-
c06aa9ec8e56
      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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 9E3FC11EE4C2767B
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
```

Deleted: 28 April

	Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 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 42007601000001904200750100000048420065010000002042006602000000040000000000000000420067020000000400000062000000004200 8E090000000800000000 4A71B8F642000D020000000400000002000000004200 0F010000009842005705000000040000000D000000004200900800000008 4B1F8ADA814C41DE42007A05000000040000000000000000420077010000006042008F07000000243232636265313433 2D666564622D343230392D386134332D6330366161396563386535360000000042000801000000284200 0A070000000C782D6174747269627574653100000000420 00B070000000656616C756531000042000F010000009842005705000000040000000D000000004200900800000008 9E3FC11EE4C2767B42007A05000000040000000000000000420077010000006042008F07000000243232636265313433 2D666564622D343230392D386134332D6330366161396563386535360000000042000801000000284200 0A070000000C782D6174747269627574653200000000420 00B070000000656616C7565320000

| 11 | Client A:
Modify attribute [batch]
In: uuidKey, attribute={ x-attribute1='ModifiedValue1' }
In: uuidKey, attribute={ x-attribute2='ModifiedValue2' }

Tag: Request Message (0x420073), Type: Structure (0x01), Data:
Tag: Request Header (0x420072), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 1C27761B124BFE06
Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56
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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 167C5332C5007D81
Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56
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

42007301000001704200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000004200 D020000000400000002000000004200 0E0000000042009008000000081C27761B124BFE06420074010000006842008F07000000243232636265313433 2D666564622D343230392D386134332D6330366161396563386535360000000042000801000000304200 0A070000000C782D6174747269627574653100000000420 00B070000000E4D6F6469666965645616C756531000042000F010000009042005705000000040000000E0000000042009008000000081C27761B124BFE06420074010000006842008F07000000243232636265313433 2D666564622D343230392D386134332D6330366161396563386535360000000042000801000000304200 0A070000000C782D617 |

Deleted: 28 April

	4747269627574653200000000042000B070000000E4D6F64696669656456616C7565320000 Out: uuidKey, attribute={ x-attribute1='ModifiedValue1' } Out: uuidKey, attribute={ x-attribute2='ModifiedValue2' } Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F7 (Thu Jul 30 17:15:03 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 1C27761B124BFE06 Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 167C5332C5007D81 Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 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 42007601000001A042007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000004A71B8F742000D020000000400000002000000042000F01000000A042005705000000040000000E000000004200900800000008167C5332C5007D8142007A0500000004000000000000000042007701000000684200 8F0700000024323263626531343 32D666564622D343230392D386134332D6330366161396563386535360000000042000801000000304200 0A070000000C782D6174747269627574653100000000042000B070000000E4D6F6469666956456616C756531000042000F01000000A042005705000000040000000E000000004200900800000008167C5332C5007D8142007A0500000004000000000000000042007701000000684200 8F0700000024323263626531343 32D6665646 22D343230392D386134332D6330366161396563386535360000000042000801000000304200 0A070000000C782D6174747269627574653200000000042000B070000000E4D6F64696669656456616C7565320000
12	Client A: Delete attribute [batch] In: uuidKey, attributeNames={ 'x-attribute1' } In: uuidKey, attributeNames={ 'x-attribute2' } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data:

Deleted: 28 April

```
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 654B7833A879B8C8
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-
c06aa9ec8e56
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 7F8D524BCE36A535
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-
c06aa9ec8e56
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2


420073010000013042007201000000384200650100000020420066020000000400000000000000004200670200000004000000620000000042000D020000000400000002000000004200F0100000070420057050000000400000000F000000004200900800000008654B7833A879B8C842007401000000484200 8F07000000243232636265313433 2D666564622D343230392D386134332D633036616139656338653536000000004200A070000000C782D6174747269627574653100000000420000F0100000007042005705000000040000000F000000004200900800000008 7F8D524BCE36A535420074010000004842008F07000000243232636265313433 2D666564622D343230392D386134332D633036616139656338653536000000004200A070000000C782D617474726962757465320000000
```

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

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

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F7 (Thu Jul 30
17:15:03 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 654B7833A879B8C8
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-
c06aa9ec8e56
      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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 7F8D524BCE36A535
```

Deleted: 28 April

	Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 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 42007601000001A042007501000000484200650100000020420066020000000400000000000000000420067020000000400000062000000004200 8E090000000800000000 4A71B8F742000D020000000400000002000000004200 0F01000000A042005705000000040000000F000000004200900800000008654B7833A879B8C842007A05000000040000000000000000042007701000000684200 8F070000002432326362653134332D666564622D343230392D386134332D6330366161396563386535360000000042000801000000304200 0A070000000C782D617474726962757465310000000042000B070000000E4D6F6469666965645645661 6C75653100004200 0F01000000A042005705000000040000000F000000004200900800000008 7F8D524BCE36A53542007A05000000040000000000000000042007701000000684200 8F070000002432326362653134332D6665646 4622D343230392D386134332D6330366161396563386535360000000042000801000000304200 0A070000000C782D6174747269627574653200000000042000B070000000E4D6F6469666965645645661 6C7565320000
13	Client A: Get (symmetric key) In: uuidKey Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 42007301000000904200720100000038420065010000002042006602000000040000000000000000042006702000000400000062000000004200 D020000000400000001000000042000F0100000048420057050000000400000000A0000000042007401000000304200 8F070000002432326362653134332D666564622D343230392D386134332D6330366161396563386535360000000042000801000000304200 0A070000000C782D6174747269627574653200000000042000B070000000E4D6F6469666965645645661 6C7565320000 Out: objectType = ‘00000002’, uuidKey, symmetricKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F7 (Thu Jul 30 17:15:03 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data:

Deleted: 28 April

	Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 Tag: Symmetric Key (0x42008A), Type: Structure (0x01), Data: Tag: Key Block (0x42003C), Type: Structure (0x01), Data: Tag: Key Value Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x42003F), Type: Structure (0x01), Data: Tag: Key Material (0x42003D), Type: Octet String (0x08), Data: 176CFFCB50904DB2AFD75D1FFF74F14F Tag: Cryptographic Algorithm (0x420025), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x420026), Type: Integer (0x02), Data: 0x00000080 (128) 42007601000001204200750100000048420065010000002042006602000000040000000000000000420067020000000400000062000000042008E090000000800000004A71B8F742000D020000000400000001000000042000F01000000C84200570500000004000000A0000000042007A0500000004000000000000000042007701000000A042005205000000040000000200000042008F070000002432326362653134332D666564622D343230392D386134332D6330366161396563386535360000000042008A010000005842003C010000005042004005000000040000000100000000420 03F010000001842003D0800000010176CFFCB50904DB2AFD75D1FFF74F14F42002505000000040000000300000000420026020000000400000008000000000
14	Client A: Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000042000D020000000400000001000000042000F0100000048420057050000000400000014000000004200740100000030 42008F070000002432326362653134332D666564622D343230392D386134332D6330366161396563386535360000000000 Out: uuidKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F8 (Thu Jul 30 17:15:04 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Deleted: 28 April

	Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 22cbe143-fedb-4209-8a43-c06aa9ec8e56 42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000000400000062000000004200 8E090000000800000000 4A71B8F842000D020000000400000001000000004200 0F010000005842005705000000040000001400000000420 07A050000000400000000000000004200770100000030420 08F0700000024323 2636265313433 2D666564622D343230392D386134332D633036616139656338653536000000000

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

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Deleted: ¶

Formatted: Indent: First line: 0 pt, Don't adjust space between Latin and Asian text

Time	Client A
0	Client A: Create (symmetric key) In: objectType = '00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', NameValue={ Name='Key1', NameType='00000001' }, CryptographicUsageMask='00000004' } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x42008D), 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:

Deleted: ObjectGroup='Group1', CryptographicAlgorithm='AES', ¶ CryptographicLength='128',¶

Deleted: 28 April

```
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420050), Type: Text String (0x07), Data: Key1
            Tag: Name Type (0x42004F), 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)


42007301000001604200720100000038420065010000002042006602000000040000000000000000420067020000000400
00006200000000042000D020000000400000001000000004200 0F0100000118420057050000000400000001000000004200
74010000010042005205000000040000000200000000042008D01000000E84200080100000003042000A0700000017437279
70746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000 3042000A07
0000001443727970746F6772617068696320 4C656E6774680000000042000B020000000400000080000000004200080100
00003842000A07000000044E616D650000000042000B0100000020420050070000000 44B6579310000000042004F050000
000400000001000000004200080100000030 42000A0700000018437279707 46F6772617068696320557361676520 4D6173
6B42000B020000000400000004000000 00
```

Out: objectType = ‘00000002’, uuidKey

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F8 (Thu Jul 30
17:15:04 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-
c51650838335


4200760100000 0C042007501000000484200650100000020420066020000000400000000000000000420067020000000400
00006200000000042008E090000000800000000 4A71B8F842000D020000000400000001000000004200 0F01000000684200
57050000000400000001000000004200 7A0500000004000000000000000004200770100000040420052050000000400000 0
020000000042008F0700000024393431316561363 42D656566372D343531322D616437352D6335313635303833383333335
00000000
```

1 Client A:

Add attribute [batch]

In: uuidKey, attribute={ ActivationDate=‘2’ }

In: uuidKey, attribute={ ProtectStopDate=’*<NOW+10min>*’ }

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
```

Deleted: 28 April

```
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 2470BEBF04DB1DAA
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-
c51650838335
      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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 7266E87E2198E367
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-
c51650838335
      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: 0x000000004A71BB50 (Thu Jul
30 17:25:04 CEST 2009)


420073010000016842007201000000384200650100000020420066020000000400000000000000004200670200000004000
0000620000000042000D020000000400000002000000004200 0F010000008842005705000000040000000D000000004200
900800000082470BEBF04DB1DAA42007401000000 6042008F0700000024393431316561363 42D656566372D343531322D
616437352D6335313635303833383333335000000004200080100000028420 00A070000000F41637469766174696F6E2044
6174650042000B0900000008000000000000000242000F0100000090420057050000000400000000D00000004200900800
0000087266E87E2198E3674200740100000 06842008F0700000024393431316561363 42D656566372D343531322D616437
352D6335313635303833383333335000000004200080100000003042000A070000001150726F746563742053746F70204461
7465000000000000000042000B0900000008000000004A71BB50
```

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

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

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8F9 (Thu Jul 30
17:15:05 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 2470BEBF04DB1DAA
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-
c51650838335
      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:
```

Deleted: 28 April

```
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Message ID (0x420090), Type: Octet String (0x08), Data: 7266E87E2198E367
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-
c51650838335
      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: 0x000000004A71BB50 (Thu Jul
30 17:25:04 CEST 2009)
```


42007601000001984200750100000048420065010000002042006602000000040000000000000000420067020000000400
0000620000000042008E090000000800000004A71B8F942000D02000000040000000200000000042000F01000000984200
5705000000004000000D00000000420090080000000082470BEBF04DB1DAA42007A0500000000400000000000000000420077
010000006042008F070000002439343131656136342D656566372D343531322D616437352D63353136353038333833335
00000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B0900000008000000000
00000242000F01000000A04200570500000000400000000D00000000420090080000000087266E87E2198E36742007A050000
0004000000000000000000420077010000006842008F070000002439343131656136342D656566372D343531322D61643735
2D633531363530383338333335000000000420008010000003042000A070000001150726F7465637420537446F7020446174
6500000000000000042000B09000000008000000004A71BB50

2 Client A:

Add Attribute

In: uuidKey, attribute={ UsageLimits={ UsageLimitsTotalBytes=‘1000’} }

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-
c51650838335
      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 (0x420094), Type: Big Integer (0x04), Data: 03E8 (1000)
```


42007301000000C84200720100000038420065010000002042006602000000040000000000000000420067020000000400
0000620000000042000D02000000040000000100000000042000F010000008042005705000000004000000D000000004200
74010000006842008F070000002439343131656136342D656566372D343531322D616437352D633531363530383338333
3500000000420008010000003042000A070000000C5573616765204C696D6974730000000042000B010000001042009404
00000008000000000000003E8

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

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
```

Deleted: 28 April

	Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8FA (Thu Jul 30 17:15:06 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335 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 (0x420094), Type: Big Integer (0x04), Data: 00000000000003E8 (1000) Tag: Usage Limits Byte Count (0x420092), Type: Big Integer (0x04), Data: 00000000000003E8 (1000) 4200760100000F84200750100000048420065010000002042006602000000040000000000000000420067020000000400 0000620000000042008E0900000008000000004A71B8FA42000D020000000400000001000000042000F01000000A04200 57050000000400000000D0000000042007A05000000040000000000000004200770100000078420008F0700000024393431 31656136342D656566372D343531322D616437352D633531363530383338333335000000004200080100000042000A07 0000000C5573616765204C696D6974730000000042000B01000000204200940400000008000000000003E84200920400 0000080000000000003E8
3	Client B: Locate (symmetric key by name) In: objectType = '00000002', attributes={ Name={ Name='Key1', NameType= '00000001'} } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420074), 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 (0x420050), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x42004F), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 4200730100000D042007201000000384200650100000020420066020000000400000000000000004200670200000004000 0000620000000042000D020000000400000001000000042000F0100000088420057050000000400000008000000004200 74010000007042000801000000284200A070000000B4F626A65637420547970650000000000042000B0500000004000000 0200000000420008010000003842000A07000000044E616D650000000042000B0100000020420050070000004B657931 0000000042004F0500000004000000100000000

Deleted: 28 April

	Out: uuidKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8FB (Thu Jul 30 17:15:07 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335 42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000004A71B8FB42000D020000000400000001000000042000F01000000584200570500000004000000080000000042007A05000000040000000000000000420077010000003042008F0700000024393431316561363 42D656566372D343531322D616437352D6335313635303833383333333500000000 Out: objectType = ‘00000002’, uuidKey, symmetricKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
4	Client B: Get (symmetric key) In: uuidKey Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335 42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000004200 0D020000000400000001000000042000F0100000048420057050000000400000000A000000004200740100000003042008F0700000024393431316561363 42D656566372D343531322D616437352D6335313635303833383333 3500000000

Deleted: 28 April

	Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8FB (Thu Jul 30 17:15:07 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335 Tag: Symmetric Key (0x42008A), Type: Structure (0x01), Data: Tag: Key Block (0x42003C), Type: Structure (0x01), Data: Tag: Key Value Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x42003F), Type: Structure (0x01), Data: Tag: Key Material (0x42003D), Type: Octet String (0x08), Data: 0ABCB1BBF5CE0CEC378DB641146C17CE Tag: Cryptographic Algorithm (0x420025), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x420026), Type: Integer (0x02), Data: 0x00000080 (128) 42007601000001204200750100000048420065010000002042006602000000040000000000000000420067020000000400000062000000004200 8E090000000800000004A71B8FB42000D020000000400000001000000004200 0F01000000C8420057050000000400000000A0000000042007A05000000040000000000000004200770100000A042005205000000040000000200000000420 08F0700000024393431316561363420656566372D343531322D616437352D6335313635303833383333350000000042008A010000005842003C0100000050420040050000000400000001000000004200 3F01000001842003D08000000100ABCB1BBF5CE0CEC378DB641146C17CE42002505000000040000000300000000420026020000000400000080000000
5	Client B: Get usage allocation In: uuidKey, UsageLimitsByteCount='500' Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335 Tag: Usage Limits Byte Count (0x420092), Type: Big Integer (0x04), Data: 01F4 (500) 42007301000000A042007201000000384200650100000020420066020000000400000000000000004200670200000004000000620000000042000D020000000400000001000000004200 0F0100000058420057050000000400000011000000004200 74010000004042008F0700000024393431316561363420656566372D343531322D616437352D6335313635303833383333350000000042009204000000080000000000001F4 Out: uuidKey, UsageLimitsByteCount='500' Tag: Response Message (0x420076), Type: Structure (0x01), Data:

Deleted: 28 April

	Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8FB (Thu Jul 30 17:15:07 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335 Tag: Usage Limits Byte Count (0x420092), Type: Big Integer (0x04), Data: 00000000000001F4 (500) 42007601000000C042007501000000484200650100000020420066020000000400000000000000004200670200000004000006200000000042008E090000000800000004A71B8FB42000D020000000400000001000000004200F01000000684200570500000004000000110000000042007A05000000040000000000000000420077010000004042008F0700000024393431316561363420656566372D343531322D616437352D6335313635303833383333350000000042009204000000080000000000001F4
6	Client A: Get usage allocation In: uuidKey, UsageLimitsByteCount='500' Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335 Tag: Usage Limits Byte Count (0x420092), Type: Big Integer (0x04), Data: 01F4 (500) 42007301000000A042007201000000384200650100000020420066020000000400000000000000004200670200000004000006200000000042000D020000000400000001000000004200F0100000058420057050000000400000011000000004200740100000042008F0700000024393431316561363420656566372D343531322D616437352D6335313635303833383333350000000042009204000000080000000000001F4 Out: uuidKey, UsageLimitsByteCount='500' Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8FB (Thu Jul 30

Deleted: 28 April

	17:15:07 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335 Tag: Usage Limits Byte Count (0x420092), Type: Big Integer (0x04), Data: 00000000000001F4 (500) 42007601000000C042007501000000484200650100000020420066020000000400000000000000000420067020000000400000062000000000420 08E0900000008000000004A71B8FB42000D020000000400000001000000000420 00F01000000684200570500000000400000011000000000420 07A05000000040000000000000000000420 07701000000404200 8F0700000024393431316561363 42D656566372D343531322D616437352D633531363530383338333335000000004200920400000008000000000000001F4
7	Client C: Locate (symmetric key by name) In: objectType = '00000002', attributes={ Name={ Name='Key1', NameType='00000001'} } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420074), 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 (0x420050), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x42004F), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007301000000D042007201000000384200650100000020420066020000000400000000000000000420067020000000400000062000000000420 0D020000000400000001000000000420 00F0100000088420057050000000400000008000000004200740100000070420008010000002842000A070000000B4F626A6563742054797065000000000042000B0500000004000000200000000420008010000003842000A07000000044E616D650000000042000B0100000020420050070000000 44B6579310000000042004F0500000004000000010000000 0 Out: uuidKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:

Deleted: 28 April

	Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8FB (Thu Jul 30 17:15:07 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335 42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000004000000062000000004200 8E090000000800000004A71B8FB42000D020000000400000001000000004200 0F01000000584200570500000004000000080000000042007A05000000040000000000000004200770100000030420 08F0700000024393431316561363420656566372D343531322D616437352D633531363530383338333333500000000
8	Client C: Get (symmetric key) In: uuidKey Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335 42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400 0006200000000042000D020000000400000001000000042000F0100000048420057050000000400000000A000000004200 7401000000304200 8F0700000024393431316561363420656566372D343531322D616437352D633531363530383338333335 00000000 Out: objectType = ‘00000002’, uuidKey, symmetricKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8FB (Thu Jul 30 17:15:07 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data:

Deleted: 28 April

	Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335 Tag: Symmetric Key (0x42008A), Type: Structure (0x01), Data: Tag: Key Block (0x42003C), Type: Structure (0x01), Data: Tag: Key Value Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x42003F), Type: Structure (0x01), Data: Tag: Key Material (0x42003D), Type: Octet String (0x08), Data: 0ABCB1BBF5CE0CEC378DB641146C17CE Tag: Cryptographic Algorithm (0x420025), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x420026), Type: Integer (0x02), Data: 0x00000080 (128) 42007601000001204200750100000048420065010000002042006602000000040000000000000000420067020000000400000062000000042008E090000000800000004A71B8FB42000D020000000400000001000000042000F01000000C8420057050000000400000000A0000000042007A0500000004000000000000000042007701000000A042005205000000040000000200000000042008F0700000024393431316561363420656566372D343531322D616437352D6335313635303833383333350000000042008A01000000584200300500000004000000010000000042003F01000000184200 3D08000000100ABCB1BBF5CE0CEC378DB641146C17CE4200250500000004000000030000000042002602000000040000008000000000
9	Client C: Get usage allocation In: uuidKey, UsageLimitsByteCount='500' Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335 Tag: Usage Limits Byte Count (0x420092), Type: Big Integer (0x04), Data: 01F4 (500) 42007301000000A042007201000000384200650100000020420066020000000400000000000000004200670200000004000000620000000042000D020000000400000001000000042000F0100000058420057050000000400000011000000004200740100000004042008F0700000024393431316561363420656566372D343531322D616437352D6335313635303833383333335000000004200920400000008000000000000001F4 Out: uuidKey, UsageLimitsByteCount='0' Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8FC (Thu Jul 30 17:15:08 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

Deleted: 28 April

	Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335 Tag: Usage Limits Byte Count (0x420092), Type: Big Integer (0x04), Data: 0000000000000000 (0) 42007601000000C0420075010000004842006501000000204200660200000004000000000000000042006702000000040000006200000000042008E090000000800000004A71B8FC42000D020000000400000001000000042000F01000000684200570500000004000000110000000042007A05000000040000000000000004200770100000042008F0700000024393431316561363420656566372D343531322D616437352D6335313635303833383333350000000042009204000000080000000000000000
10	Client A: Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335 42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000004200D020000000400000001000000042000F0100000048420057050000000400000014000000042007401000000304200F0700000024393431316561363420656566372D343531322D616437352D6335313635303833383333335000000042 Out: uuidKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8FC (Thu Jul 30 17:15:08 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: 9411ea64-eef7-4512-ad75-c51650838335

Deleted: 28 April

	42007601000000B042007501000000484200650100000020420066020000000400000000000000000420067020000000400 00006200000000042008E0900000008000000004A71B8FC42000D020000000400000001000000004200F01000000584200 57050000000400000014000000042007A0500000004000000000000000042007701000000304200 8F0700000024393431 31656136342D656566372D343531322D616437352D6335313635303833383333500000000

6 Key Interchange, Key Exchange

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

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

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.

Formatted: Indent: First line: 0 pt

Time	Request/Response messages

0	Register (symmetric key)
	In: objectType = '00000002', attributes={ CryptographicUsageMask='00000004' }, foreignSymmetricKey
	
	Tag: Request Message (0x420073), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000003 (Register)
	  Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
	  Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
	  Tag: Template-Attribute (0x42008D), 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 (0x42008A), Type: Structure (0x01), Data:
	  Tag: Key Block (0x42003C), Type: Structure (0x01), Data:
	  Tag: Key Value Type (0x420040), Type: Enumeration (0x05), Data: 0x00000001
	  Tag: Key Value (0x42003F), Type: Structure (0x01), Data:
	  Tag: Key Material (0x42003D), Type: Octet String (0x08), Data: 0123456789ABCDEF0123456789ABCDEF
	  Tag: Cryptographic Algorithm (0x420025), Type: Enumeration (0x05), Data: 0x00000003 (AES)
	  Tag: Cryptographic Length (0x420026), Type: Integer (0x02), Data: 0x00000080 (128)
	
	42007301000001104200720100000038420065010000002042006602000000040000000000000000420067020000000400000062000000004200 D020000000400000001000000004200F01000000C84200570500000004000000080000000042007401000000B042005205000000040000000200000000042008D0100000038420008010000003042000A0700000018437

Deleted: 28 April

	27970746F6772617068696320557361676520 4D61736B42000B0200000004000000040000000042008A01000000584200 3C0100000050420040050000000400000001000000042003F0100000018420 03D0800000010012345678 9ABCDEF0123456789ABCDEF4200250500000004000000030000000042002602000000040000008000000000 Out: objectType = '00000002', uuidKey Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8FC (Thu Jul 30 17:15:08 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000003 (Register) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Object Type (0x420052), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: efc9e72e-6922-4b36-8651-f91a69924358 42007601000000C042007501000000484200650100000020420066020000000400000000000000000420067020000000400000062000000004200 8E090000000800000000 4A71B8FC42000D020000000400000001000000004200 0F010000006842005705000000040000000300000000042007A05000000040000000000000000420077010000004042005205000000040000002000000004200 8F07000000246566633965373265 2D363932322D346233362D383635312D663931613639393234333538000000000
1	Add attribute In: uuidKey, attribute={ x-provider='unknown' } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: efc9e72e-6922-4b36-8651-f91a69924358 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 42007301000000C042007201000000384200650100000020420066020000000400000000000000000420067020000000400000062000000004200 0D020000000400000001000000004200 0F010000007842005705000000040000000D0000000042007401000000006042008F07000000246566633965373265 2D363932322D346233362D383635312D663931613639393234333538000000000420008010000002842000A070000000A782D70726F7669646572000000000000420000B0700000007756E6B6E6F776E00

Deleted: 28 April

	Out: uuidKey, attribute={ x-provider='unknown' } Tag: Response Message (0x420076), Type: Structure (0x01), Data: Tag: Response Header (0x420075), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98) Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8FD (Thu Jul 30 17:15:09 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: efc9e72e-6922-4b36-8651-f91a69924358 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 42007601000000E042007501000000484200650100000020420066020000000400000000000000004200670200000004000000620000000042008E090000000800000004A71B8FD42000D020000000400000001000000004200F010000008842005705000000040000000D0000000042007A05000000040000000000000000420077010000006042008F0700000024656663396537326523633932322D346233362D383635312D663931613639393234333538000000004200080100000028420004A070000000A782D70726F766964657200000000000042000B0700000007756E6B6E6F776E00
2	Modify attribute In: uuidKey, attribute={ x-provider='third party' } Tag: Request Message (0x420073), Type: Structure (0x01), Data: Tag: Request Header (0x420072), Type: Structure (0x01), Data: Tag: Protocol Version (0x420065), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Request Payload (0x420074), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: efc9e72e-6922-4b36-8651-f91a69924358 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 42007301000000C842007201000000384200650100000020420066020000000400000000000000004200670200000004000000620000000042000D020000000400000001000000004200F0100000080420057050000000400000000E000000004200741000000068420080F07000000246566633965373265 2D363932322D346233362D383635312D663931613639393234333538000000004200801000000284200A070000000A782D70726F766964657200000000000042000B070000000B7468697264207061727479000000000000 Out: uuidKey, attribute={ x-provider='third party' }

Deleted: 28 April

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8FD (Thu Jul 30
17:15:09 CEST 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x420077), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: efc9e72e-6922-4b36-8651-
f91a69924358
      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


42007601000000E84200750100000048420065010000002042006602000000040000000000000000420067020000000400
0000062000000004200 8E090000000800000004A71B8FD42000D020000000400000001000000004200 0F010000009042
00570500000004000000 0E0000000042007A05000000040000000000000000420077010000006842008F0700000024656
66339653732652D363932322D346233362D383635312D663931613639393234333538000000004200080100000030420 0
0A070000000A782D70726F766964657200000000000042000B070000000B7468697264207061727479000000000000
```

3 Destroy (symmetric key)

In: uuidKey

```
Tag: Request Message (0x420073), Type: Structure (0x01), Data:
  Tag: Request Header (0x420072), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), 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 (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420074), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: efc9e72e-6922-4b36-8651-
f91a69924358


42007301000000904200720100000038420065010000002042006602000000040000000000000000420067020000000400
0000062000000004200 0D020000000400000001000000004200 0F010000004842005705000000040000001400000000042
00740100000030 42008F0700000024656663396537326 52D363932322D346233362D383635312D6639316136393932343
3353800000000
```

Out: uuidKey

```
Tag: Response Message (0x420076), Type: Structure (0x01), Data:
  Tag: Response Header (0x420075), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420065), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x420066), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x420067), Type: Integer (0x02), Data: 0x00000062 (98)
    Tag: Time Stamp (0x42008E), Type: Date-Time (0x09), Data: 0x000000004A71B8FD (Thu Jul 30
```

Deleted: 28 April

	17:15:09 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x420057), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007A), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420077), Type: Structure (0x01), Data: Tag: Unique Identifier (0x42008F), Type: Text String (0x07), Data: efc9e72e-6922-4b36-8651-f91a69924358 42007601000000B042007501000000484200650100000020420066020000000400000000000000004200670200000000400000062000000004200 8E090000000800000004A71B8FD42000D020000000400000001000000004200 0F010000005842005705000000040000001400000000420 07A050000000400000000000000004200770100000030420 08F0700000024656663396536 52652D363932322D346233362D383635312D663931613639393234333538000000000

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', CriticalityIndicator='false', VendorExtension={ tag='0x42014242', type='text string', value='na' } } Out: objectType='00000002', uuidKey
1	Destroy (symmetric key) In: uuidKey Out: uuidKey

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt

Deleted: ¶

Deleted: 12

Deleted: 28 April

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='000000**0C**' }, MessageExtension={ VendorIdentification='Acme', CriticalityIndicator='true', VendorExtension={ tag='0x42014242', 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='000000**0C**' }, privateKeyAttributes={ Name={ NameValue='PrivateKey1', NameType='00000001' } }, publicKeyAttributes={ NameValue='PublicKey1', NameType='00000001' } } 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

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt

Deleted: 12

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt

Deleted: 12

Deleted: 28 April

	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='000000**0C**' }, foreignPrivateKey Out: uuidPrivateKey
1	Register (Public Key) In: objectType='00000004', attributes={ CryptographicUsageMask='000000**0C**', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } }, foreignPublicKey Out: uuidPublicKey
2	Add attribute In: uuidPrivateKey, attribute={ Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } } Out: uuidPrivateKey, attribute={ Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } }
3	Locate (Public Key) In: attributes={ objectType='PublicKey', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } } Out: uuidPublicKey
4	Locate (Private Key) In: attributes={ objectType='PrivateKey', Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } } Out: uuidPrivateKey
5	Destroy In: uuidPrivateKey Out: uuidPrivateKey
6	Destroy In: uuidPublicKey Out: uuidPublicKey

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt

Deleted: 12

Deleted: 12

Deleted: 28 April

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 can still be retrieved. To clean up, both keys are deleted.

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

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt

Deleted: ¶

Deleted: 00000012’

Deleted: 28 April

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* should be set in the past and the *Deactivation Date* in the near future. Repeated Get Attribute calls are performed to verify that the state is first "Active", then subsequently "Deactive". Then issue a Re-key request, including an *Activation Date* attribute with the value set to the previously specified *Deactivation Date* of the existing key. Verify from the response that the *Activation Date* and *Deactivation Date* attributes were set correctly (if they are not returned, issue a Get Attribute request). Do a Get Attribute operation to verify that the state of the new key is "Active". To clean up, both keys are deleted.

Time	Client A
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C' } Out: objectType='00000002', uuidKey
1	Add Activation Date, Deactivation Date attributes based on Timestamp in previous response (batch) In: uuidKey, attribute={ ActivationDate=' <*Timestamp in previous response – 365 days*>' } In: uuidKey, attribute={ DeactivationDate='<*Timestamp in previous response + 2 minutes*>' } Out: uuidKey, attribute={ ActivationDate=' <*Timestamp in previous response - 1 year*>' } Out: uuidKey, attribute={ DeactivationDate=' <*Timestamp in previous response + 2 minutes*>' }
2	Get Attribute * *Repeated until state changes to Deactivated* In: uuidKey, attributeName={'State'} Out: uuidKey, attribute={ State='*Active*' }
3	Get Attribute In: uuidKey, attributeName={'State'} Out: uuidKey, attribute={ State='*Deactive*' }
4	Rekey In: uuidKey, attribute={ offset='018B8200' *(300 days)*} Out: uuidNewKey
5	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

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt

Deleted: 12

Deleted: 28 April

	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 will be copied from the existing key. Do a Get Attribute operation to verify that the state of the new key is "Active". To clean up, both keys are deleted.

Time	Client A
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', 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
5	Get Attribute In: uuidNewKey, attributeName={'State'} Out: uuidNewKey, attribute={ State='*Active*' }
6	Destroy In: uuidKey Out: uuidKey
7	Destroy In: uuidNewKey Out: uuidNewKey

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt

Deleted: ¶

Deleted: 12

Deleted: 28 April

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

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

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

9.5 Use-case: Obtain Lease for Expired Key

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

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

Deleted: 12

Deleted: 28 April

	Out: uuidKey	
10	Destroy In: uuidNewKey Out: uuidNewKey	

10 Archival

These use-cases test archiving and locating keys using the off-line indicator. The Archive and Recover operations may be performed asynchronously, in which case the client must Poll the server until the operations complete. The client must also indicate in the request that it supports asynchronous responses.

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

Create a symmetric key with a specified name, then use Locate to find the key and get the key. Archive the key (asynchronous operation, use Poll until it completes) and use Get and Locate on it, but both should fail. Add the Storage Status Mask to the Locate-command, indicating that the server should search in both online and archived storage. The Locate finds the key. Recover the key from the archive (also asynchronous), both Locate and Get succeed.

Time	Client A
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='archiveKey', NameType='00000001' } } Out: objectType='00000002', uuidKey
1	Locate In: attributes={ Name={ NameValue='archiveKey', NameType='00000001' } } Out: uuidKey
2	Get (symmetric key) In: uuidKey Out: objectType = '00000002', uuidKey, symmetricKey
3	Archive In: uuidKey, asynchronousIndicator='true' Out: asynchronousCorrelationValue
4	Poll* In: asynchronousCorrelationValue Out: uuidKey
5	Get (symmetric key) In: uuidKey Out: Operation Failed, Item Not Found
6	Locate

Formatted: Indent: Left: 0 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: Left: 0 pt

Deleted: ¶

Deleted: 12

Deleted: 28 April

	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: 28 April

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: 28 April

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.

Deleted: 28 April