



# Key Management Interoperability Protocol Use Cases Version 1.0

Committee Draft 0509 / Public Review 0102

~~05 November 2009~~

18 March 2010

## Specification URIs:

### This Version:

- <http://docs.oasis-open.org/kmip/usecases/v1.0/cd09/kmip-usecases-1.0-cd-09.html>
- <http://docs.oasis-open.org/kmip/usecases/v1.0/cd09/kmip-usecases-1.0-cd-09.doc> (Authoritative)
- <http://docs.oasis-open.org/kmip/usecases/v1.0/cd09/kmip-usecases-1.0-cd-09.pdf>

### Previous Version:

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

### Previous Version:

N/A

### Latest Version:

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

## Technical Committee:

OASIS Key Management Interoperability Protocol (KMIP) TC

### Chair(s):

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

### Editor(s):

Mathias Björkqvist, IBM <[mbj@zurich.ibm.com](mailto:mbj@zurich.ibm.com)>  
René Pawlitzek, IBM <[rpa@zurich.ibm.com](mailto:rpa@zurich.ibm.com)>

### Related work:

This specification replaces or supersedes:

- None

This specification is related to:

- [Key Management Interoperability Protocol Specification Version 1.0](#)
- [Key Management Interoperability Protocol Profiles Version 1.0](#)
- [Key Management Interoperability Protocol Usage Guide Version 1.0](#)

### Abstract:

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

Style Definition: Heading 3,H3,h3,Level 3  
Topic Heading: Font color: Auto

Style Definition: Heading 4,H4,h4,First  
Subheading: Font color: Auto

Style Definition: Heading 5,h5,Second  
Subheading: Font color: Auto

Style Definition: Heading 6,h6,Third  
Subheading: Font color: Auto

Style Definition: Heading 7,DON'T USE 7:  
Font color: Auto

Style Definition: Heading 8, DON'T USE 8:  
Font color: Auto

Style Definition: Heading 9, DON'T USE 9:  
Font color: Auto

Style Definition: AppendixHeading3: Font  
color: Auto

Field Code Changed

Formatted: Default Paragraph Font

Field Code Changed

Field Code Changed

Formatted: Default Paragraph Font

Field Code Changed

Formatted: Default Paragraph Font

Field Code Changed

Formatted: Default Paragraph Font

Field Code Changed

Formatted: Default Paragraph Font

Field Code Changed

Formatted: Default Paragraph Font

Field Code Changed

Field Code Changed

Field Code Changed

**Status:**

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

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

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

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

## Notices

Copyright © OASIS® ~~2009-2010~~. All Rights Reserved.

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

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

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

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

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

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

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

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

# Table of Contents

1	Introduction	4
	Table of Contents	
1.1	Normative References	6
	1 Introduction	
2	Message exchange	6
	1.1 Normative References	
3	Centralized Management	6
	2 Message exchange	
3.1	Basic functionality	7
	3 Centralized Management	
3.1.1	Use-case: Create / Destroy Basic functionality	7
3.1.2	1 Use-case: Register / Create / Get attributes / Destroy	7
3.1.3	2 Use-case: Register / Create / Locate / Get attributes / Destroy	9
3.1.4	3 Use-case: Dual client use-case, ID Placeholder linked Create / Locate & / Get batch/ Destroy	16
3.2	1.4 Use-case: Asynchronous Dual client use-case, ID Placeholder linked Locate & Get batch	22
4	Key life cycle support	39
	3.1.5 Use-case: Register / Destroy Secret Data	
4.1	3.2 Use-case: Revoke scenario Asynchronous Locate	41
5	Auditing and reporting	53
	4 Key life cycle support	
5.1	Use-case: Get usage allocation Revoke scenario	53
6	Key Interchange, Key Exchange	73
	5 Auditing and reporting	
6.1	Use-case: Import of a Third-party Key Get usage allocation scenario	73
7	Vendor Extensions	88
	6 Key Interchange, Key Exchange	
7.1	Use-case: Unrecognized Message Extension with Criticality Indicator false Import of a Third-party Key	88
7.2	Use-case: Unrecognized Message Extension with Criticality Indicator true	88
	7 Vendor Extensions	
		93

- Formatted: Style Heading 1h1Level 1 Topic Heading + Before: 5 pt After: 5...
- Formatted: Don't adjust space between Latin and Asian text, Tab stops: Not at 24 pt
- Field Code Changed ... [1]
- Formatted: TOC 1,toc1, Don't adjust space between Latin and Asian text, Tab stops: Not at 48 pt
- Field Code Changed ... [2]
- Formatted: TOC 2,toc2, Don't adjust space between Latin and Asian text, Tab stops: Not at 24 pt
- Field Code Changed ... [3]
- Field Code Changed ... [4]
- Formatted: TOC 1,toc1, Don't adjust space between Latin and Asian text, Tab stops: Not at 48 pt
- Field Code Changed ... [5]
- Formatted: TOC 2,toc2, Don't adjust space between Latin and Asian text, Tab stops: Not at 60 pt
- Field Code Changed ... [6]
- Field Code Changed ... [7]
- Field Code Changed ... [8]
- Field Code Changed ... [9]
- Formatted: TOC 3,toc3, Don't adjust space between Latin and Asian text, Tab stops: Not at 48 pt
- Field Code Changed ... [10]
- Formatted: TOC 3,toc3, Don't adjust space between Latin and Asian text, Tab stops: Not at 24 pt
- Field Code Changed ... [11]
- Formatted ... [12]
- Field Code Changed ... [13]
- Formatted ... [14]
- Field Code Changed ... [15]
- Formatted ... [16]
- Field Code Changed ... [17]
- Formatted ... [18]
- Field Code Changed ... [19]
- Formatted ... [20]
- Field Code Changed ... [21]
- Formatted ... [22]
- Field Code Changed ... [23]
- Formatted ... [24]
- Field Code Changed ... [25]
- Field Code Changed ... [26]



# 1 Introduction

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

8  
9 The use-cases define a number of client-to-server request-response pairs for a number of operations. For  
10 each request-response message pair the operation is stated, along with the relevant parameters needed  
11 for the request or response message. This is followed by two different illustrations of the messages: first,  
12 a human-readable construction which shows the fields tags, types and values, followed by the TTLV-  
13 encoding of the message. These are included to facilitate the implementation of the message creation  
14 and parsing functionality. The use-cases show one possible way to construct the messages, and the  
15 messages shown are not necessarily the only correct constructions (e.g. it is possible to omit the attribute  
16 index if it is zero). Also note that many values change dynamically when running the use-cases (the  
17 server-generated timestamps, Unique Identifiers and key material in responses, as well as Batch Item ID  
18 values in client-generated requests).

19 [In many situations in the use cases defined in this document, the server behavior depends on the server's](#)  
20 [policy. The illustrated message exchanges and their contents are not the only possible variants \(see](#)  
21 [\[KMIP-Spec\]](#)). E.g., the server response messages shown in this document correspond to a server policy

22 [of completely destroying a managed object, along with all of its attributes, when receiving a Destroy](#)  
23 [request.](#)  
24 [Multiple use cases describe several clients operating on the same managed object\(s\). For this to work,](#)  
25 [the clients SHALL have authenticated themselves to the server using the same credentials \(see \[KMIP-](#)  
26 [Prof\]\). Alternatively, the server policy applied to the relevant managed object\(s\) SHALL be such that the](#)  
27 [clients all have access to the managed object\(s\) in question.](#)

## 28 4.1.1 Normative References

- 29 **[KMIP-Spec]** OASIS Committee Draft [0610](#), *Key Management Interoperability Protocol*  
30 *Specification Version 1.0, November 2009*. [http://docs.oasis-](http://docs.oasis-open.org/kmip/spec/v1.0/ed06/kmip-spec-1.0-cd-06.doc)  
31 [open.org/kmip/spec/v1.0/ed06/kmip-spec-1.0-cd-06.doc](http://docs.oasis-open.org/kmip/spec/v1.0/ed06/kmip-spec-1.0-cd-06.doc) Mar 2010,  
32 <http://docs.oasis-open.org/kmip/spec/v1.0/ed10/kmip-spec-1.0-cd-10.doc>
- 33 **[KMIP-Prof]** OASIS Committee Draft [0405](#), *Key Management Interoperability Protocol Profiles*  
34 *Version 1.0, November 2009* Mar 2010,  
35 [http://docs.oasis-open.org/kmip/profiles/v1.0/ed04cd05/kmip-profiles-1.0-cd-](http://docs.oasis-open.org/kmip/profiles/v1.0/ed04cd05/kmip-profiles-1.0-cd-0405.doc)  
36 [0405.doc](http://docs.oasis-open.org/kmip/profiles/v1.0/ed04cd05/kmip-profiles-1.0-cd-0405.doc)

## 38 2.2 Message exchange

39 The message exchange between clients and the server to test the following use-case scenarios is  
40 performed with TTLV encoding over the [http transport](#). ~~This is to facilitate debugging and to focus on~~  
41 ~~KMIP specific issues instead of potential secure transport setup problems.~~ [TLS/SSL transport as defined](#)  
42 [in \[KMIP-Spec\] and \[KMIP-Prof\]](#).

Formatted: Outline numbered + Level: 1 +  
Numbering Style: 1, 2, 3, ... + Start at: 1 +  
Alignment: Left + Aligned at: 0 pt + Indent at:  
0 pt, Don't adjust space between Latin and  
Asian text

Formatted: Outline numbered + Level: 2 +  
Numbering Style: 1, 2, 3, ... + Start at: 1 +  
Alignment: Left + Aligned at: 0 pt + Indent at:  
0 pt, Don't adjust space between Latin and  
Asian text

Formatted: Font: Not Bold

Formatted: Ref term

Formatted: Ref term

Formatted: Ref term, Font: Not Bold

Formatted: Ref term

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

Formatted: Ref term

Field Code Changed

Formatted: Style Heading 1h1Level 1 Topic  
Heading + Before: 5 pt After: 5..., Outline  
numbered + Level: 1 + Numbering Style: 1, 2,  
3, ... + Start at: 2 + Alignment: Left + Aligned  
at: 0 pt + Indent at: 0 pt

## 44 **33** Centralized Management

### 45 **3.4.3.1** Basic functionality

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

#### 49 **3.4.3.1.1** Use-case: Create / Destroy

50 In this use-case the client issues a Create request, whereby the server creates a new symmetric key and  
51 returns the Unique Identifier. To clean up, the client then performs a Destroy operation to destroy the key.  
52

Formatted: Style Heading 1h1Level 1 Topic  
Heading + Before: 5 pt After: 5..., Outline  
numbered + Level: 1 + Numbering Style: 1, 2,  
3, ... + Start at: 2 + Alignment: Left + Aligned  
at: 0 pt + Indent at: 0 pt

Formatted: Indent: Left: 0 pt, Outline  
numbered + Level: 2 + Numbering Style: 1, 2,  
3, ... + Start at: 1 + Alignment: Left + Aligned  
at: 36 pt + Indent at: 36 pt, Don't adjust  
space between Latin and Asian text

Formatted: Font: Not Bold

Formatted: Outline numbered + Level: 3 +  
Numbering Style: 1, 2, 3, ... + Start at: 1 +  
Alignment: Left + Aligned at: 0 pt + Indent at:  
0 pt, Don't adjust space between Latin and  
Asian text

Formatted: Font: Not Bold, Font color: Custom  
Color(RGB(59,0,111))

Time	Request/Response messages
0	<p>Create (symmetric key)</p> <p>In: objectType='00000002' (Symmetric Key), attributes={ CryptographicAlgorithm='00000003' (AES), CryptographicLength='128', CryptographicUsageMask='0000000C' }</p> <p>Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)</p> <p>Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:</p> <p>Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</p> <p>Tag: Template-Attribute (0x42008E0x420091), Type: Structure (0x01), Data:</p> <p>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm</p> <p>Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)</p> <p>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length</p> <p>Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)</p> <p>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask</p> <p>Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)</p> <p>42007501000001204200740100000038420067010000002042006802000000400000001000000004200690200000004 0000000000000042000B0200000040000001000000042000F01000000842005A050000004000000100000000 42007601000000C042005505000000400000002000000042008E01000000A8420008010000003042000A0700000017 43727970746F6772617068696320416C676F72697468690042000B0500000040000000300000004200080100000030 42000A070000001443727970746F67726170686963204C655E677468000000042000B020000004000000000000000 42008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004 000000C00000000</p> <p>42007801000001204200770100000038420069010000002042006A020000004000000010000000042006B0200000004</p>

0000000000000042000D0200000040000001000000042000F0100000D842005C05000000400000010000000  
4200790100000C0420057050000004000000200000004200910100000A842000801000003042000A070000017  
43727970746F6772617068696320416C676F726974686D004200B050000004000000300000000420008010000030  
42000A07000001443727970746F67726170686963204C656E677468000000042000B020000004000000800000000  
42000801000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B020000004  
0000000C00000000

Out: objectType='00000002', uuidKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0731C (Mon  
Sep 28 10:26:04 CEST0x000000004AFBE7C2 (Thu Nov 12 11:47:30 CET 2009)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric  
Key)  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 46eea90a-4b20-  
423e-b968-750f299f0ea7fc8833de-70d2-4ece-b063-fede3a3c59fe

42007801000000C04200770100000048420067010000002042006802000000400000001000000004200690200000004  
00000000000000042008F090000000800000004AC0731C42000D020000004000000010000000042000F0100000068  
42005A0500000004000000010000000042007E05000000040000000000000042007901000000404200550500000004  
000000020000000420091070000002434366563613930612D346232302D343233632D623936382D3735306632393966  
30636137000000042007B01000000C042007A0100000048420069010000002042006A020000004000000010000000  
42006B020000004000000000000004200920900000008000000004AFBE7C242000D0200000040000000100000000  
42000F010000006842005C050000004000000010000000042007F05000000400000000000000042007C0100000040  
420057050000004000000020000000042009407000000246663383833364652D373064322D346563652D623036332D  
66656465336133633539666500000000

1 Destroy (symmetric key)  
In: uuidKey

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 46eea90a-4b20-  
423e-b968-750f299f0ea7fc8833de-70d2-4ece-b063-fede3a3c59fe

42007501000000004200740100000038420067010000002042006802000000400000001000000004200690200000004  
00000000000000042008F090000000800000004AC0731C42000D020000004000000010000000042000F0100000068  
42005A0500000004000000010000000042007E05000000040000000000000042007901000000404200550500000004  
4200760100000030420091070000002434366563613930612D346232302D343233632D623936382D3735306632393966



3063613700000000

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D020000004000000010000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002466633838333364652D373064322D346563652D623036332D66656465336133633539666500000000

Out: uuidKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
 Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
 Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
 Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0731D (Mon Sep 28 10:26:05 CEST 2009)  
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
 Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
 Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
 Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
 Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 46eea90a-4b20-423e-b968-750f299f0ea7fc8833de-70d2-4ece-b063-fede3a3c59fe

42007801000000B0420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042000D02000000040000000040000000040000000042000F0100000004842005C050000000400000014000000004200790100000030420094070000002466633838333364652D373064322D346563652D623036332D6665646533613363353966650000000042007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000000420092090000008000000004AFBE7C342000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F05000000040000000000000042007C0100000030420094070000002466633838333364652D373064322D346563652D623036332D66656465336133633539666500000000

53  
54  
55  
56  
57  
58  
59

**3.1.23.1.2 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:** Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0 pt + Indent at: 0 pt, Don't adjust space between Latin and Asian text

**Formatted:** Font: Not Bold, Font color: Custom Color(RGB(59,0,111))

Time	Request/Response messages
0	Register (template) In: objectType='00000007', attributesTemplateAttribute=empty, Template={ ObjectGroup='Group1', ApplicationSpecificInformation='ssl, www.example.com', ContactInformation='Joe', x-Purpose='demonstration', Name={ NameValue='Template1', NameType='00000001' } }  Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data: Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000006 (Template)  
Tag: Template-Attribute (0x42008E0x420091), Type: Structure (0x01), Data: null  
Tag: Template (0x420090), Type: Structure (0x01), Data:  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group  
Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Application Specific Information  
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:  
Tag: Application Namespace (0x420003), Type: Text String (0x07), Data: ssl  
Tag: Application Data (0x420002), Type: Text String (0x07), Data: www.example.com  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information  
Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-Purpose  
Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: demonstration  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name  
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:  
Tag: Name Value (0x4200530x420055), Type: Text String (0x07), Data: Template1  
Tag: Name Type (0x4200520x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

-----  
42007501000001c0420074010000003842006701000000204200680200000004000000010000000042006902000000040  
00000000000004200000200000004000000010000000042000F010000017842005A050000004000000030000000042  
0076010000016042005505000000400000006000000042008E0100000148420008010000002842000A070000000C4F6  
26A6563742047726F7570000000042000B07000000647726F7570310000420008010000005842000A07000000204170  
706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000B010000002842000307000000373736  
C00000000420002070000000F777772E6578616D706C652E636F6D00420008010000003042000A0700000013436F6E  
7461637420496E666F726D6174696F6E00000000042000B07000000034A6F6500000000420008010000003042000A0  
700000009782B507572706F736500000000000042000B070000000D64656D6F6E7374726174696F6E00000042000801  
0000004042000A07000000044E616D65000000042000B0100000028420053070000000954656D706C6E1746531000000  
000000042005205000000040000000100000000

42007801000001C84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040  
0000000000000042000D0200000004000000010000000042000F010000018042005C0500000004000000030000000042  
00790100000168420057050000000400000006000000042009101000000042009001000001484200080100000028420  
00A070000000C4F626A6563742047726F7570000000042000B070000000647726F757031000042000801000000584200  
0A07000000204170706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000B010000002842000  
3070000000373736C000000000420002070000000F777772E6578616D706C652E636F6D00420008010000003042000A  
0700000013436F6E7461637420496E666F726D6174696F6E00000000042000B07000000034A6F650000000004200080  
10000003042000A0700000009782B507572706F736500000000000042000B070000000D64656D6F6E7374726174696F  
6E000000420008010000004042000A07000000044E616D65000000042000B0100000028420055070000000954656D706  
C6174653100000000000042005405000000040000000100000000

Out: uuidTemplate

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:

Formatted: Font color: Black

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
 Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC0731E (Mon Sep 28 10:26:06 CEST 2009)  
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
 Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)  
 Tag: Result Status (0x42007C0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
 Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
 Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fe3ff473-4de4-4248-990e-21e00f7fe006a6ebbb6f-4c54-4bbb-ad29-be6bad4ecad5

42007801000000B0420077010000004842006701000000204200680200000040000000100000004200690200000040000000000042008F090000000800000004AC0731E42009D0200000040000000100000004200F010000005842005A050000004000000030000000042007C050000000400000000000000420079010000003042009107000000243466632366343732D346465342D343234382D393930652D323165303066376663303036000000042007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000420092090000000800000004AFBE7C442000D02000000400000001000000042000F010000005842005C050000004000000030000000042007F05000000040000000000000042007C010000003042009407000000246136656262636662D346335342D34626262D616432392D62653662616434656361643500000000

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

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
 Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
 Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
 Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
 Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
 Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
 Tag: Template-Attribute (0x42008E0x420091), Type: Structure (0x01), Data:  
 Tag: Name (0x4200510x420053), Type: Structure (0x01), Data:  
 Tag: Name Value (0x4200530x420055), Type: Text String (0x07), Data: Template1  
 Tag: Name Type (0x4200520x420054), 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)

4200750100000150420074010000003842006701000000204200680200000040000000100000004200690200000040  
000000000000042000D0200000004000000010000000042000F010000010842005A0500000004000000010000000042  
007601000000F0420055050000000400000002000000042008E01000000D842005101000000284200530700000009546  
56D706C61746531000000000000042005205000000040000000100000000420008010000003042000A07000000174372  
7970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000  
A070000001443727970746F67726170686963204C656E6774680000000042000B0200000004000000800000000420008  
010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000  
C00000000

42007801000001504200770100000038420069010000002042006A0200000004000000010000000042006B0200000040  
000000000000042000D0200000004000000010000000042000F010000010842005C0500000004000000010000000042  
007901000000F04200570500000004000000020000000042009101000000D842005301000000284200550700000009546  
56D706C61746531000000000000042005405000000040000000100000000420008010000003042000A07000000174372  
7970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000  
A070000001443727970746F67726170686963204C656E6774680000000042000B0200000004000000800000000420008  
010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000  
C00000000

Out: objectType='0000002', uuidKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:

Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0731F (Mon Sep 28 10:26:07 CEST 2009)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)

Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:

Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 300881e8-596a-48ad-814f-7ee1198966861b10614-d8b5-46f9-8d17-2fa6eald747a

42007801000000C0420077010000004842006701000000204200680200000040000000100000004200690200000040  
000000000000042008F090000000800000004AC0731F42000D0200000004000000010000000042000F010000006842  
005A0500000004000000010000000042007C05000000040000000000000042007901000000404200550500000004000  
0000200000000420091070000002433303038383163382D353936612D343861642D383134662D37636531313938393636  
3038000000042007B01000000C042007A01000000048420069010000002042006A0200000004000000010000000042006  
B0200000004000000000000004200920900000008000000004AFBE7C542000D02000000400000001000000042000F  
010000006842005C0500000004000000010000000042007F05000000040000000000000042007C01000000404200570  
50000000400000002000000004200940700000002436316231303631342D643862352D343666392D386431372D32666136  
656131643734376100000000

2	<p>Get attributes</p> <p>In: uuidKey, attributeNames={'ObjectGroup', 'ApplicationSpecificInformation', 'ContactInformation', 'x-Purpose'}</p> <p>Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p>
---	---

Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 300881e8-596a-48ad-814f-7ce11989660861b10614-d8b5-46f9-8d17-2fa6eald747a  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Application Specific Information  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-Purpose

420075010000001084200740100000038420067010000002042006802000000400000001000000042006902000000040000000000042000D020000004000000010000000042000F01000000C042005A0500000040000000B0000000042007601000000A8420091070000002433303038383163382D353936612D343861642D383134662D376365313139383936363038000000042000A070000000C4F626A6563742047726F75700000000042000A07000000204170706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000A0700000013436F6E7461637420496E666F726D6174696F6E00000000042000A0700000009782D507572706F736500000000000000  
420078010000001084200770100000038420069010000002042006A02000000400000001000000042006B020000000400000000000042000D020000004000000010000000042000F01000000C042005C0500000040000000B0000000042007901000000A8420094070000002436316231303631342D643862352D343666392D386431372D326661366561316437343761000000042000A070000000C4F626A6563742047726F75700000000042000A07000000204170706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000A0700000013436F6E7461637420496E666F726D6174696F6E00000000042000A0700000009782D507572706F736500000000000000

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

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC0731F (Mon Sep 28 10:26:07 CEST 2009)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
Tag: Result Status (0x42007C0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 300881e8-596a-48ad-814f-7ce11989660861b10614-d8b5-46f9-8d17-2fa6eald747a  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group  
Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Application Specific Information  
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:  
Tag: Application Namespace (0x420003), Type: Text String (0x07), Data: ssl  
Tag: Application Data (0x420002), Type: Text String (0x07), Data: www.example.com  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:

Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information  
 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe  
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-Purpose  
 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: demonstration

420078010000001B0420077010000004842006701000000204200680200000040000000100000004200690200000040  
 000000000000042008F09000000000000004AC0731F42000D02000000400000001000000042000F010000015842  
 005A05000000040000000000000042007C0500000004000000000000000042007901000001304200910700000024333  
 03028383163382D353936612D343861642D383134662D376365313139383936363038000000042000801000000284200  
 0A070000000C4F626A6563742047726F7570000000042000B070000000647726F7570310000420008010000005842000  
 A07000000204170706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000B0100000028420003  
 070000000373736C0000000000420002070000000F777772E6578616D706C652E636F6D00420008010000003042000A0  
 700000013436F6E7461637420496E666F726D6174696F6E00000000042000B07000000034A6F6500000000042000801  
 0000003042000A0700000009782D507572706F7365000000000000042000B070000000D64656D6F6E7374726174696F6  
 E0000042007B01000001B042007A0100000048420069010000002042006A020000004000000010000000042006B0200  
 0000040000000000000004200920900000008000000004AFBE7C642000D0200000004000000010000000042000F01000  
 0015842005C05000000040000000B0000000042007F05000000040000000000000042007C0100000130420094070000  
 002436316231303631342D643862352D343666392D386431372D326661366561316437343761000000042000801000000  
 02842000A0700000000C4F626A6563742047726F7570000000042000B070000000647726F757031000042000801000000  
 5842000A07000000204170706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000B010000002  
 8420003070000000373736C000000000420002070000000F777772E6578616D706C652E636F6D004200080100000030  
 42000A07000000013436F6E7461637420496E666F726D6174696F6E000000000042000B07000000034A6F650000000004  
 20008010000003042000A0700000009782D507572706F736500000000000042000B070000000D64656D6F6E73747261  
 74696F6E000000

3 Destroy (symmetric key)  
 In: uuidKey

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
 Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
 Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
 Tag: Operation (0x420095A0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
 Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
 Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 300881e8-596a-48ad-814f-7ce11989660861b10614-d8b5-46f9-8d17-2fa6eald747a

4200750100000090420074010000003842006701000000204200680200000040000000100000004200690200000040  
 000000000000042008D0200000004000000010000000042000F010000004842005A05000000400000014000000042  
 00760100000030420091070000002433303038383163382D353936612D343861642D383134662D3763653131393839363  
 6303800000000

42007801000000904200770100000038420069010000002042006A02000000400000001000000042006B0200000040  
 000000000000042000D02000000400000001000000042000F010000004842005C05000000400000014000000042  
 00790100000030420094070000002436316231303631342D643862352D343666392D386431372D3266613665613164373  
 4376100000000

Out: uuidKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
 Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
 Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor ([0x4200690x42006B](#)), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp ([0x42008F0x420092](#)), Type: Date-Time (0x09), Data: [0x000000004AC07320 \(Mon Sep 28 10:26:08 CEST 2009\)](#)

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

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

Tag: Operation ([0x42005A0x42005C](#)), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

Tag: Result Status ([0x42007E0x42007F](#)), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload ([0x4200790x42007C](#)), Type: Structure (0x01), Data:

Tag: Unique Identifier ([0x4200910x420094](#)), Type: Text String (0x07), Data: [300881e8-596a-48ad-814f-7ee11989660861b10614-d8b5-46f9-8d17-2fa6eald747a](#)

[42007801000000004200770100000048420067010000002042006802000000040000000100000000420069020000000400000000000042008F090000000800000004AC0732042009D0200000040000000100000004200F010000005842005A05000000400000014000000042007C05000000040000000000000000004200790100000030420091070000002433303038383163382D353936612D343861642D383134662D3763653131393839363630380000000042007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000000000420092090000008000000004AFBE7C64200D0200000040000000100000004200F010000005842005C05000000400000014000000042007F05000000040000000000000042007C0100000030420094070000002436316231303631342D643862352D343666392D386431372D32666136656131643734376100000000](#)

4 Destroy (template)

In: uuidTemplate

Tag: Request Message ([0x4200750x420078](#)), Type: Structure (0x01), Data:

Tag: Request Header ([0x4200740x420077](#)), Type: Structure (0x01), Data:

Tag: Protocol Version ([0x4200670x420069](#)), Type: Structure (0x01), Data:

Tag: Protocol Version Major ([0x4200680x42006A](#)), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor ([0x4200690x42006B](#)), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation ([0x42005A0x42005C](#)), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

Tag: Request Payload ([0x4200760x420079](#)), Type: Structure (0x01), Data:

Tag: Unique Identifier ([0x4200910x420094](#)), Type: Text String (0x07), Data: [4fe3f473-4de4-4248-990e-21e00f7fe006a6ebbb6f-4c54-4bbb-ad29-be6bad4ecad5](#)

[42007501000000004200740100000038420067010000002042006802000000040000000100000000420069020000000400000000000042008F090000000800000004AC0732042009D0200000040000000100000004200F010000005842005A05000000400000014000000042007C050000000400000000000000000042007901000000304200910700000024346663336633437332D346465342D343234382D393930652D32316530306637666330303600000000](#)

[42007801000000004200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000000420092090000008000000004AFBE7C64200D0200000040000000100000004200F010000005842005C05000000400000014000000042007F05000000040000000000000042007C0100000030420094070000002461366562626236662D346335342D346262622D616432392D62653662616434656361643500000000](#)

Out: uuidTemplate

Tag: Response Message ([0x4200780x42007B](#)), Type: Structure (0x01), Data:

Tag: Response Header ([0x4200770x42007A](#)), Type: Structure (0x01), Data:

Tag: Protocol Version ([0x4200670x420069](#)), Type: Structure (0x01), Data:

Tag: Protocol Version Major ([0x4200680x42006A](#)), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor ([0x4200690x42006B](#)), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp ([0x42008F0x420092](#)), Type: Date-Time (0x09), Data: [0x000000004AC07320 \(Mon Sep 28 10:26:08 CEST 2009\)](#)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

Tag: Result Status (0x4200760x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fe3f473-4de4-4248-990e-21e00f7fe006a6ebbb6f-4c54-4bbb-ad29-be6bad4ecad5

4200780100000000B0420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042008F0900000000000000004AC0732042000D0200000004000000010000000042000F0100000005842005A0500000004000000014000000042007C0500000004000000000000004200790100000030420091070000002434666332663437332D346465342D343234382D393930652D3231653030663766633030360000000042007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000000420092090000008000000004AFBE7C642000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002461366562626236662D346335342D346262622D616432392D62653662616434656361643500000000

60  
61  
62  
63  
64  
65  
66  
67

### 3.1.33.1.3 Use-case: Create / Locate / Get / Destroy

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

**Formatted:** Outline numbered + Level: 3 +  
Numbering Style: 1, 2, 3, ... + Start at: 1 +  
Alignment: Left + Aligned at: 0 pt + Indent at:  
0 pt, Don't adjust space between Latin and  
Asian text

**Formatted:** Font: Not Bold, Font color: Custom  
Color(RGB(59,0,111))

Time	Request/Response messages
0	<p>Create (symmetric key)</p> <p>In: objectType = '00000002', attributes={ Name={ NameValue='Key1', NameType='00000001' }, CryptographicAlgorithm='DES', CryptographicLength='56', CryptographicUsageMask='0000000C', ContactInformation='Joe' }</p> <p>Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)</p> <p>Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:</p> <p>Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</p> <p>Tag: Template-Attribute (0x42008E0x420091), Type: Structure (0x01), Data:</p> <p>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name</p> <p>Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:</p> <p>Tag: Name Value (0x4200530x420055), Type: Text String (0x07), Data: Key1</p> <p>Tag: Name Type (0x4200520x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)</p> <p>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm</p>



Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: [0x00000001](#)  
[\(DES0x00000002 \(3DES\)\)](#)

Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length  
Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: [0x00000038](#) ([560x000000A8](#)  
[\(168\)](#))

Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage  
Mask

Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt,  
Decrypt)

Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information  
Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe

[4200750100000198420074010000003842006701000000204200680200000040000000100000004200690200000040](#)  
[00000000000042000D02000000400000001000000042000F010000015042005A050000004000000010000000042](#)  
[00760100000138420055050000000400000002000000042008B0100000120420008010000003842000A07000000044E6](#)  
[16D65000000042000B010000002042005307000000044B657931000000042005205000000400000001000000004200](#)  
[08010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B05000000400000](#)  
[00100000000420008010000003042000A070000001443727970746F6772617068696320416C676F726974686D0042000B](#)  
[0200000004000000380000000420008010000003042000A070000001843727970746F677261706869632055736167652](#)  
[04D61736B42000B0200000040000000C00000000420008010000003042000A0700000013436F6E7461637420496E666F](#)  
[726D6174696F6E00000000042000B07000000034A6F650000000000](#)

[42007801000001984200770100000038420069010000002042006A0200000004000000010000000042006B02000000040](#)  
[000000000000042000D020000004000000010000000042000F010000015042005C0500000004000000010000000042](#)  
[0079010000013842005705000000040000000200000004200910100000120420008010000003842000A07000000044E6](#)  
[16D65000000042000B010000002042005507000000044B6579310000000420054050000000400000001000000004200](#)  
[08010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B0500000004000000](#)  
[00200000000420008010000003042000A070000001443727970746F6772617068696320416C676F726974686D0042000B](#)  
[0200000004000000A800000000420008010000003042000A070000001843727970746F677261706869632055736167652](#)  
[04D61736B42000B0200000040000000C00000000420008010000003042000A0700000013436F6E7461637420496E666F](#)  
[726D6174696F6E00000000042000B07000000034A6F650000000000](#)

Out: objectType = '00000002', uuidKey

Tag: Response Message ([0x4200780x42007B](#)), Type: Structure (0x01), Data:  
Tag: Response Header ([0x4200770x42007A](#)), Type: Structure (0x01), Data:  
Tag: Protocol Version ([0x4200670x420069](#)), Type: Structure (0x01), Data:  
Tag: Protocol Version Major ([0x4200680x42006A](#)), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor ([0x4200690x42006B](#)), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp ([0x42008F0x420092](#)), Type: Date-Time (0x09), Data: [0x00000004AC07321](#) ([Mon Sep 28 10:26:09 CEST0x00000004AFBE7C7](#) (Thu Nov 12 11:47:35 CET 2009))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation ([0x42005A0x42005C](#)), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
Tag: Result Status ([0x42007E0x42007F](#)), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload ([0x4200790x42007C](#)), Type: Structure (0x01), Data:  
Tag: Object Type ([0x4200550x420057](#)), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Unique Identifier ([0x4200910x420094](#)), Type: Text String (0x07), Data: [75da9be9-7867-49e5-886d-757f3d523d3f1ed28ea5-2b31-4145-bcf2-36d0756d3890](#)

[4200780100000004200770100000048420067010000002042006802000000400000001000000004200690200000040](#)  
[00000000000042008F090000000800000004AC0732142000D020000004000000010000000042000F010000006842](#)  
[005A050000000400000001000000042007C050000000400000000000004200790100000040420055050000004000](#)  
[0000200000000420091070000002437356461396263392D373836372D343963352D383836642D37353766336435323364](#)

3366000000042007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000420092090000000800000004AFBE7C742000D0200000040000001000000042000F010000006842005C050000000400000001000000042007F05000000040000000000000042007C0100000040420057050000004000000020000000420094070000002431656432386561352D326233312D343134352D62636632D3336643037353664333839300000000

1

Locate (symmetric key)  
In: attributes={ objectType = '0000002', Name={ Name='Key1', NameType='0000001' } }

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Request Payload (0x4200760x420079), 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 (0x4200530x420055), Type: Text String (0x07), Data: Key1  
Tag: Name Type (0x4200520x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

4200750100000000420074010000003842006701000000204200680200000004000000010000000420069020000000400000000000042000D02000000040000000000000042000F010000008842005A05000000040000000800000004200760100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000000000420008010000003842000A0700000044E616D65000000042000B010000002042005307000000044B6579310000000042005205000000040000000100000000

42007801000000D04200770100000038420069010000002042006A020000000400000001000000042006B0200000004000000000000042000D020000000400000001000000042000F010000008842005C05000000040000000800000004200790100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000000000420008010000003842000A0700000044E616D65000000042000B010000002042005507000000044B6579310000000042005405000000040000000100000000

Out: uuidKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC07321 (Mon Sep 28 10:26:09 CEST 2009)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

	<p>Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: <a href="#">75da9be9-7867-49e5-886d-757f3d523d3f1ed28ea5-2b31-4145-bcf2-36d0756d3890</a></p> <p><a href="#">42007801000000004200770100000004842006701000000204200680200000004000000010000000420069020000000400000000000042008F090000000000000004AC0732142000D02000000400000001000000042000F010000005842005A050000000400000000000000042007C05000000040000000000000004200790100000030420091070000002437356461396263392D373836372D343963352D383836642D37353766336435323643366000000042007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000000420092090000008000000004AFBE7C842000D020000004000000010000000042000F010000005842005C050000000400000008000000042007F050000000400000000000000042007C0100000030420094070000002431656432386561352D326233312D343134352D626366322D33366430373536643338393000000000</a></p>
2	<p><b>Get (symmetric key)</b></p> <p>In: uuidKey</p> <p>Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)</p> <p>Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: <a href="#">75da9be9-7867-49e5-886d-757f3d523d3f1ed28ea5-2b31-4145-bcf2-36d0756d3890</a></p> <p><a href="#">42007501000000004200740100000038420067010000002042006802000000040000000100000004200690200000004000000000000042000D0200000004000000010000000042000F010000004842005A05000000040000000A000000004200760100000030420091070000002437356461396263392D373836372D343963352D383836642D37353766336435323643366000000000</a></p> <p><a href="#">42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002431656432386561352D326233312D343134352D626366322D33366430373536643338393000000000</a></p> <p>Out: objectType = '00000002', uuidKey, symmetricKey</p> <p>Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:</p> <p>Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: <del>0x00000004AC07322 (Mon Sep 28 10:26:10 CEST 0x00000004AFBE7C8 (Thu Nov 12 11:47:36 CET 2009)</del></p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)</p> <p>Tag: Result Status (0x42007C0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</p> <p>Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:</p> <p>Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</p> <p>Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: <a href="#">75da9be9-7867-</a></p>

	<p><a href="#">49e5-886d-757f3d523d3f1ed28ea5-2b31-4145-bcf2-36d0756d3890</a></p> <p>Tag: Symmetric Key (<a href="#">0x420080x42008F</a>), Type: Structure (0x01), Data:</p> <p>Tag: Key Block (<a href="#">0x42003E0x420040</a>), Type: Structure (0x01), Data:</p> <p>Tag: Key Format Type (<a href="#">0x4200400x420042</a>), Type: Enumeration (0x05), Data: 0x00000001</p> <p>Tag: Key Value (<a href="#">0x4200430x420045</a>), Type: Structure (0x01), Data:</p> <p>Tag: Key Material (<a href="#">0x4200410x420043</a>), Type: Octet String (0x08), Data: <a href="#">EAD09734B085DFFC8E51523F73D6EE9F40EAB7CD06825499D8C0BD0739E1046</a></p> <p>Tag: Cryptographic Algorithm (<a href="#">0x4200260x420028</a>), Type: Enumeration (0x05), Data: 0x00000001 (<a href="#">DE90x00000002 (3DES)</a>)</p> <p>Tag: Cryptographic Length (<a href="#">0x4200280x42002A</a>), Type: Integer (0x02), Data: <a href="#">0x00000038 (560x000000A8 (168))</a></p> <p><a href="#">420078010000001184200770100000048420067010000002042006802000000400000001000000042006902000000400000000000042008F09000000800000004AC0732242000D02000000400000001000000042000F01000000C042005A0500000040000000A000000042007C0500000040000000000000042007901000000984200550500000040000000000000420091070000002437356461396263392D373836372D343963352D383836642D373537663364353233643366000000420080010000005042003E01000000484200400500000040000000100000004200430100000010420041080000008EAD09734B085DFFC8E51523F73D6EE9F40EAB7CD06825499D8C0BD0739E104642002802000000400000038000000042007B010000012842007A0100000048420069010000002042006A02000000400000001000000042006B0200000040000000000000042009209000000800000004AFBE7C842000D02000000400000001000000042000F01000000D042005C0500000040000000A000000042007F05000000040000000000000042007C01000000A8420057050000004000000020000000420094070000002431656432386561352D326233312D343134352D626366322D33366430373536643338393000000042008F0100000060420040010000005842004205000000400000001000000042004501000000204200430800000018C8E51523F73D6EE9F40EAB7CD06825499D8C0BD0739E10464200280500000040000002000000042002A0200000040000000A800000000</a></p>
3	<p><b>Destroy (symmetric key)</b></p> <p>In: <code>uuidKey</code></p> <p>Tag: Request Message (<a href="#">0x4200750x420078</a>), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (<a href="#">0x4200740x420077</a>), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (<a href="#">0x4200670x420069</a>), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (<a href="#">0x4200680x42006A</a>), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (<a href="#">0x4200690x42006B</a>), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (<a href="#">0x42005A0x42005C</a>), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</p> <p>Tag: Request Payload (<a href="#">0x4200760x420079</a>), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (<a href="#">0x4200910x420094</a>), Type: Text String (0x07), Data: <a href="#">75da9be9-7867-49e5-886d-757f3d523d3f1ed28ea5-2b31-4145-bcf2-36d0756d3890</a></p> <p><a href="#">420075010000000904200740100000038420067010000002042006802000000400000001000000042006902000000400000000000042008002000000400000001000000042000F010000004842005A0500000040000001400000004200760100000030420091070000002437356461396263392D373836372D343963352D383836642D37353766336435323364336600000000</a></p> <p><a href="#">42007801000000904200770100000038420069010000002042006A02000000400000001000000042006B0200000040000000000000042000D02000000400000001000000042000F010000004842005C0500000040000001400000004200790100000030420094070000002431656432386561352D326233312D343134352D626366322D33366430373536643338393000000000</a></p> <p>Out: <code>uuidKey</code></p> <p>Tag: Response Message (<a href="#">0x4200780x42007B</a>), Type: Structure (0x01), Data:</p> <p>Tag: Response Header (<a href="#">0x4200770x42007A</a>), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (<a href="#">0x4200670x420069</a>), Type: Structure (0x01), Data:</p>

Tag: Protocol Version Major ([0x4200680x42006A](#)), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor ([0x4200690x42006B](#)), Type: Integer (0x02), Data: 0x00000000 (0)  
 Tag: Time Stamp ([0x42008F0x420092](#)), Type: Date-Time (0x09), Data: ~~0x00000004AC07322 (Mon Sep 28 10:26:10 CEST 2009)~~ [0x00000004AFBE7C8 \(Thu Nov 12 11:47:36 CET 2009\)](#)  
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
 Tag: Operation ([0x42005A0x42005C](#)), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
 Tag: Result Status ([0x4200760x42007F](#)), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
 Tag: Response Payload ([0x4200790x42007C](#)), Type: Structure (0x01), Data:  
 Tag: Unique Identifier ([0x4200910x420094](#)), Type: Text String (0x07), Data: ~~75da9be9-7867-49e5-886d-757f3d523d3f1ed28ea5-2b31-4145-bcf2-36d0756d3890~~  
[42007801000000B842007701000000384200670100000020420068020000004000000010000000420069020000004000000000000042008F090000008000000004AC0732242000D0200000040000000100000004200F010000005842005A05000000400000014000000042007C05000000400000004000000000004200790100000030420091070000002437356461396263392D373836372D343963352D383836642D373537663364353233643366000000042007B01000000B042007A0100000048420069010000002042006A02000000400000001000000042006B02000000400000000000000042009209000000800000004AFBE7C842000D0200000040000000100000004200F010000005842005C050000004000000014000000042007F050000004000000000000042007C0100000030420094070000002431656432386561352D32623312D343134352D626366322D3336643037353664333839300000000](#)

4

**Locate**  
 In: uuidKey

Tag: Request Message ([0x4200750x420078](#)), Type: Structure (0x01), Data:  
 Tag: Request Header ([0x4200740x420077](#)), Type: Structure (0x01), Data:  
 Tag: Protocol Version ([0x4200670x420069](#)), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major ([0x4200680x42006A](#)), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor ([0x4200690x42006B](#)), Type: Integer (0x02), Data: 0x00000000 (0)  
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
 Tag: Operation ([0x42005A0x42005C](#)), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
 Tag: Request Payload ([0x4200760x420079](#)), 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: ~~75da9be9-7867-49e5-886d-757f3d523d3f1ed28ea5-2b31-4145-bcf2-36d0756d3890~~

[42007501000000B84200740100000038420067010000002042006802000000400000001000000042006902000000400000000000042008F010000008000000040000000100000004200F010000005842005A050000004000000000000042007C05000000400000004000000000004200790100000030420091070000002437356461396263392D373836372D343963352D383836642D373537663364353233643366000000042007B01000000B042007A0100000048420069010000002042006A02000000400000001000000042006B02000000400000000000000042009209000000800000004AFBE7C842000D0200000040000000100000004200F010000005842005C05000000400000000000000042007F050000004000000000000042007C0100000030420094070000002431656432386561352D32623312D343134352D626366322D3336643037353664333839300000000](#)

Out: <empty response payload>

Tag: Response Message (0x420078), Type: Structure (0x01), Data:  
 Tag: Response Header (0x420077), Type: Structure (0x01), Data:  
 Tag: Protocol Version (0x420067), Type: Structure (0x01), Data:

```

Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x42008F), Type: Date-Time (0x09), Data: 0x000000004AC07323 (Mon Sep 28
10:26:11 CEST 2009)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x420079), Type: Structure (0x01), Data: null

42007801000000008042007701000000484200670100000020420068020000004000000010000000042006902000000040
000000000000042008F0900000008000000004AC0732342000D020000004000000010000000042000F010000002842
005A050000000400000008000000042007C05000000040000000000000420079010000000042007B01000000080420
07A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000004200
920900000008000000004AFBE7C842000D0200000004000000010000000042000F010000002842005C050000000400000
00800000000042007F0500000000400000000000000042007C0100000000

```

68  
69

70 **3-1.43.1.4 Use-case: Dual client use-case, ID Placeholder linked Locate & Get**  
71 **batch**

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

78  
79 This use-case demonstrates the fact that it is possible for two clients to cooperate and use the same  
80 managed object while only having knowledge of a single pre-agreed Name attribute value and without  
81 having to share any other information. Here, the identities of the two clients are not considered and since  
82 we do not include an Authentication field in the header, they could also be considered to be the same  
83 client. If the clients authenticate themselves to the server using different credentials, the server needs to  
84 employ another policy than the Default policy defined in the KMIP specification on the key object to allow  
85 both clients to access it.  
86

**Formatted:** Outline numbered + Level: 3 +  
Numbering Style: 1, 2, 3, ... + Start at: 4 +  
Alignment: Left + Aligned at: 0 pt + Indent at:  
0 pt, Don't adjust space between Latin and  
Asian text

**Formatted:** Font: Not Bold, Font color: Custom  
Color(59,0,111)

Time	Request/Response messages
0	<p>Client A: Register (template)</p> <p>In: objectType='00000007', attributesTemplateAttribute=empty, Template={ CryptographicAlgorithm='AES', CryptographicLength='128', Name={ NameValue='Template1', NameType='00000001' },}</p> <p>Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data: Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p>

Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000006 (Template)  
Tag: Template-Attribute (0x42008E0x420091), Type: Structure (0x01), Data: null  
Tag: Template (0x420090), Type: Structure (0x01), Data:  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm  
Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length  
Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name  
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:  
Tag: Name Value (0x4200530x420055), Type: Text String (0x07), Data: Template1  
Tag: Name Type (0x4200520x420054), Type: Enumeration (0x05), Data: 0x00000001  
(Uninterpreted text string)

-----  
420075010000001304200740100000038420067010000002042006802000000400000001000000004200690200000040  
00000000000004200000200000004000000010000000042000F01000000E842005A0500000004000000030000000042  
007601000000D04200550500000004000000060000000042008E01000000B8420008010000003042000A0700000017437  
27970746F6772617068696320416C676F726974686D0042000B050000000400000003000000042000801000000304200  
0A070000001443727970746F6772617068696320416C676F726974686D0042000B050000000400000003000000042000  
8010000004042000A07000000044E616D65000000042000B0100000028420053070000000954656D706C617465310000  
00000000042005205000000040000000100000000  
42007801000001384200770100000038420069010000002042006A0200000004000000010000000042006B0200000040  
0000000000000042000D0200000004000000010000000042000F01000000F042005C0500000004000000030000000042  
007901000000D84200570500000004000000060000000042009101000000042009001000000B84200080100000030420  
00A070000001743727970746F6772617068696320416C676F726974686D0042000B05000000040000000300000004200  
08010000003042000A070000001443727970746F6772617068696320416C676F726974686D0042000B020000000400000  
0800000000420008010000004042000A07000000044E616D65000000042000B0100000028420055070000000954656D  
706C61746531000000000000042005405000000040000000100000000

Formatted: Font color: Black

Out: uuidTemplate

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC07323 (Mon Sep 28 0x00000004AFBED21 (Thu Nov 12 12:10:26+11 CEST 2009))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)  
Tag: Result Status (0x42007C0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 8383198b-4600-4388-955f-2802ee699e9e45d8629a-9ad1-41b3-9d09-941f2a595da3

42007801000000B04200770100000048420067010000002042006802000000400000001000000004200690200000040  
0000000000000420008F09000000000000004AC073234200902000000400000001000000042000F01000000E842  
005A050000000400000003000000042007C05000000040000000000000042007901000000304200910700000024383

33833313938622b343630302b343338382b393535662b3238303263633639396539630000000042007B0100000B04200  
7A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000000042009  
20900000008000000004AFBED2142000D0200000004000000010000000042000F010000005842005C050000000400000  
030000000042007F050000000400000000000000042007C0100000030420094070000002434356438363239612D39616  
4312D343162332D396430392D39343166326135393564613300000000

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

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric  
Key)  
Tag: Template-Attribute (0x42008E0x420091), Type: Structure (0x01), Data:  
Tag: Name (0x4200510x420053), Type: Structure (0x01), Data:  
Tag: Name Value (0x4200530x420055), Type: Text String (0x07), Data: Template1  
Tag: Name Type (0x4200520x420054), 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 (0x4200530x420055), Type: Text String (0x07), Data: Key1  
Tag: Name Type (0x4200520x420054), 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

42007501000001584200740100000003842006701000000204200680200000004000000010000000042006902000000040  
000000000000042000D0200000004000000010000000042000F010000011042005A0500000004000000010000000042  
007601000000F84200550500000004000000020000000042008E01000000E042005101000000284200530700000009546  
56D706C61746531000000000000042005205000000040000000100000000420008010000003842000A07000000044E61  
6D650000000042000B010000002042005307000000044B657931000000004200520500000004000000010000000042000  
8010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000  
0400000000420008010000003042000A0700000013436F6E7461637420496E66F726D6174696FE00000000042000B0  
700000003466F6F0000000000

42007801000001584200770100000038420069010000002042006A0200000004000000010000000042006B02000000040  
000000000000042000D0200000004000000010000000042000F010000011042005C0500000004000000010000000042  
007901000000F84200570500000004000000020000000042009101000000E042005301000000284200550700000009546  
56D706C6174653100000000000042005405000000040000000100000000420008010000003842000A07000000044E61  
6D650000000042000B010000002042005507000000044B657931000000004200540500000004000000010000000042000  
8010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000



040000000420008010000003042000A0700000013436F6E7461637420496E666F726D6174696F6E0000000004200B070000003466F6F0000000000

Out: objectType='00000002', uuidKey

Tag: Response Message (0x420070x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC07324 (Mon Sep 28 0x000000004AFBED23 (Thu Nov 12 12:10:26+12-CST27 CET 2009))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3c2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

420078010000000420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000042008F0900000000000000004AC073242008D020000000400000001000000004200F010000006842005A0500000004000000010000000042007C05000000040000000000000004200790100000040420055050000000400000000000420091070000002437666261303834392D613363322D346438632D383164642D3961313939343765343764000000042007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004AFBED2342000D020000000400000001000000004200F010000006842005C050000000400000001000000042007F05000000040000000000000042007C01000000404200570500000004000000020000000420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961653300000000

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 (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: 01F76942FF5A7A8A0E9E1875336E415E  
Tag: Request Payload (0x4200760x420079), 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 (0x4200530x420055), Type: Text String (0x07), Data: Key1  
Tag: Name Type (0x4200520x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: 3192EBD439D59CC4CFEF21DDDF1CF5E3  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data: null

4200750100000120420074010000004842006701000000204200680200000040000000100000004200690200000004000000000000420010060000008000000000000000142000D02000000400000002000000042000F010000009842005A05000000400000008000000042009308000000801F76942FF5A7A8A420076010000007042000801000000284200A070000000B4F626A656374205479706500000000042000B050000004000000020000000420008010000003842000A07000000044E616D65000000042000B010000002042005307000000044B6579310000000420052050000004000000010000000042000F010000002842005C05000000040000000A00000000420093080000008CFEF21DDDF1CF5E34200760100000000

42007801000001204200770100000048420069010000002042006A02000000400000001000000042006B0200000004000000000000420010060000008000000000000000142000D02000000400000002000000042000F010000009842005C0500000040000000800000004200930800000080E9E1875336E415E420079010000007042000801000000284200A070000000B4F626A656374205479706500000000042000B050000004000000020000000420008010000003842000A07000000044E616D65000000042000B010000002042005507000000044B65793100000004200540500000040000000010000000042000F010000002842005C05000000040000000A00000000420093080000008CFEF21DDDF1CF5E34200790100000000

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

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC07324 (Mon Sep 0x000000004AFBED24 (Thu Nov 12 12:10:28 10+26+12-CEST CET 2009))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: 01F76942FF5A7A8A0E9E1875336E415E  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-8idd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: 3192EBD439D59CC4CFEF21DDDF1CF5E3  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:

Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

Tag: Symmetric Key (0x420080x42008F), Type: Structure (0x01), Data:

Tag: Key Block (0x42003E0x420040), Type: Structure (0x01), Data:

Tag: Key Format Type (0x4200400x420042), Type: Enumeration (0x05), Data: 0x00000001

Tag: Key Value (0x4200430x420045), Type: Structure (0x01), Data:

Tag: Key Material (0x4200410x420043), Type: Octet String (0x08), Data: 5c7b76dc93ef45fd9231522eb2ce7b0a755d03c639648fb5828d5f1cc9fe9b57

Tag: Cryptographic Algorithm (0x4200260x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)

Tag: Cryptographic Length (0x4200280x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

420078010000001A0420077010000004842006701000000204200680200000040000000100000000420069020000000400000000000042008F09000000000000000000000000420091070000002437666261303834392d613363322d346438632d383164642d3961313939393437653437640000000042009F01000000B842005A05000000040000000A00000000420090080000000083192EBD439D59CE442007C05000000400000000000000042007901000000A0420055050000004000000020000000420091070000002437666261303834392d613363322d346438632d383164642d396131393939343765343764000000042008C010000005842003E0100000050420040050000000400000010000000420043010000001842004108000000105c7b76dc93ef45fd9231522eb2ce7b0a420026050000000400000003000000042002802000000400000080000000042007B01000001A042007A010000048420069010000002042006A020000000400000001000000042006B020000004000000000000042009209000000800000004AFBED244200D0200000040000000200000004200F010000006842005C0500000040000000800000004200930800000080E9E1875336E415E42007F0500000040000000000000042007C010000003042009407000000243061333653833652D356237612D343836352D393634612D386431633362626639616533000000042000F010000000D842005C0500000040000000A00000000420093080000008CFEF21DDDF1CF5E342007F050000004000000000000000042007C01000000A042005705000000400000002000000042009407000000243061333653833652D356237612D343836352D393634612D386431633362626639616533000000042008F0100000058420040010000005042004205000000040000001000000004200450100000018420043080000010755D03C639648FB5828D5F1CC9FE9B57420028050000000400000030000000042002A0200000040000008000000000

3 Client B:  
Get attribute list  
In: uuidKey

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

4200750100000009042007401000000384200670100000020420068020000004000000010000000042006902000000040000000000000042008F09000000000000000000000000420091070000002437666261303834392d613363322d346438632d383164642d39613139393934376534376400000000

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042009209000000800000004AFBED244200D0200000040000000200000004200F010000006842005C0500000040000000800000004200930800000080E9E1875336E415E42007F0500000040000000000000042007C010000003042009407000000243061333653833652D356237612D343836352D393634612D386431633362626639616533000000042000F010000000D842005C0500000040000000A00000000420093080000008CFEF21DDDF1CF5E342007F050000004000000000000000042007C01000000A042005705000000400000002000000042009407000000243061333653833652D356237612D343836352D393634612D386431633362626639616533000000042008F0100000058420040010000005042004205000000040000001000000004200450100000018420043080000010755D03C639648FB5828D5F1CC9FE9B57420028050000000400000030000000042002A0200000040000008000000000



Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information

420075010000000004200740100000038420067010000002042006802000000040000000100000000420069020000000400000000000042000D02000000040000000910000000042000F010000007842005A0500000040000000B000000004200760100000060420091070000002437666261303834392D613363322D346438632D383164642D3961313939393437653437640000000042000A07000000044E616D65000000042000A0700000013436F6E7461637420496E666F726D6174696F6E0000000000

420078010000000004200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000007842005C05000000040000000B000000004200790100000060420094070000002430613333653833652D356237612D343836352D393634612D386431633362626639616533000000042000A07000000044E616D65000000042000A0700000013436F6E7461637420496E666F726D6174696F6E0000000000

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

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC07325 (Mon Sep 0x000000004AFBED24 (Thu Nov 12 12:10:28 +0+26+13 -CEST CET 2009))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
Tag: Result Status (0x42007C0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name  
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:  
Tag: Name Value (0x4200530x420055), Type: Text String (0x07), Data: Key1  
Tag: Name Type (0x4200520x420054), 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

4200780100000128420077010000004842006701000000204200680200000040000000100000004200690200000040  
000000000000042008F09000000000000004AC0732542000D02000000400000001000000042000F010000000042  
005A0500000040000000B0000000042007C0500000004000000000000042007901000000A84200910700000024376  
66261303834392D613363322D346438532B383164642D396131393939343765343764000000042000801000000384200  
0A07000000044E616D65000000042000B010000002042005307000000044B6579310000000420052050000000400000  
00100000000420008010000003042000A0700000013436F6E7461637420496E666F726D6174696F6E00000000042000B  
0700000003466F6F00000000042007B010000012842007A0100000048420069010000002042006A0200000040000000  
10000000042006B0200000040000000000000042009209000000800000004AFBED2442000D02000000400000001  
0000000042000F01000000D042005C05000000040000000B0000000042007F0500000040000000000000042007C010  
00000A8420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961653300  
000000420008010000003842000A0700000044E616D65000000042000B01000000204200507000000044B657931000  
000004200540500000004000000010000000420008010000003042000A0700000013436F6E7461637420496E666F726D  
6174696F6E00000000042000B0700000003466F6F0000000000

5

Client B:

Add attribute [batch]

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

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

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200660x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)

Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: 290C75CAE59F39087A92DDA525EB158A

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

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

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

Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value1

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)

Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: BF48C307C95CC22E7230F6E4D3BEA249

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

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

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

Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value2

4200750100000160420074010000003842006701000000204200680200000040000000100000004200690200000040  
000000000000042000D02000000400000002000000042000F010000008842005A05000000400000000000000042  
009008000000008290C75CAE59F39084200760100000060420091070000002437666261303834392D613363322D3464386  
32D383164642D3961313939393437653437640000000420008010000002842000A070000000C782D6174747269627574  
6531000000042000B070000000656616C756531000042000F010000008842005A05000000400000000000000042009  
0800000008BF48C307C95CC22E4200760100000060420091070000002437666261303834392D613363322D346438632D  
383164642D3961313939393437653437640000000420008010000002842000A070000000C782D6174747269627574653  
2000000042000B070000000656616C7565320000

42007801000001604200770100000038420069010000002042006A02000000400000001000000042006B0200000040  
000000000000042000D02000000400000002000000042000F010000008842005C0500000040000000D0000000042

00930800000087A92DDA525EB158A4200790100000060420094070000002430613333653833652D356237612D3438363  
52D393634612D3864316333626266396165330000000420008010000002842000A070000000C782D6174747269627574  
6531000000042000B070000000656616C75653100004200F010000008842005C050000000400000000D0000000042009  
30800000087230F6E4D3BEA2494200790100000060420094070000002430613333653833652D356237612D343836352D  
393634612D3864316333626266396165330000000420008010000002842000A070000000C782D6174747269627574653  
20000000042000B070000000656616C7565320000

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

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

Tag: Response Message (0x4200700x42007B), Type: Structure (0x01), Data:

Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200640x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC07326 (Mon Sep 28 0x000000004AFBED25 (Thu Nov 12 12:10:26+14 CEST29 CET 2009))

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)

Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: 290c75cae59f39087a92dda525eb158a

Tag: Result Status (0x42007e0x42007f), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x4200790x42007c), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-8idd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

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

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

Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value1

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)

Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: BF48c307c95cc22e7230f6e4d3bea249

Tag: Result Status (0x42007e0x42007f), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x4200790x42007c), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-8idd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

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

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

Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value2

42007801000001904200770100000048420067010000002042006802000000040000000100000000420069020000000040  
000000000000042008F090000000800000004AC073264200D0200000040000000200000004200F010000009842  
005A05000000040000000D00000004200900800000008290c75cae59f390842007c050000000400000000000000420  
0790100000060420091070000002437666261303834392D61336322D346438632D383164642D39613139393934376534  
376400000000420008010000002842000A070000000C782D617474726962757465310000000042000B070000000656616  
C756531000042000F010000009842005C05000000040000000D00000000420099080000008BF48c307c95cc22e42007c  
050000004000000000000004200790100000060420091070000002437666261303834392D61336322D346438632D3  
83164642D3961313939393437653437640000000420008010000002842000A070000000C782D61747472696275746532  
0000000042000B070000000656616C756532000042007B010000019042007A0100000048420069010000002042006A020  
0000004000000010000000042006802000000400000000000000042009209000000800000004AFBED2542000D0200  
00004000000020000000042000F010000009842005C0500000040000000D000000004200930800000087A92DDA525E  
B158A42007F05000000040000000000000042007C0100000060420094070000002430613333653833652D356237612D  
343836352D393634612D3864316333626266396165330000000420008010000002842000A070000000C782D617474726  
962757465310000000042000B070000000656616C756531000042000F010000009842005C0500000040000000D000000  
004200930800000087230F6E4D3BEA24942007F05000000400000000000000042007C010000006042009407000000

430613333653833652D356237612D343836352D393634612D38643163336266396165330000000420008010000028  
42000A070000000C782D61747472696275746532000000042000B070000000656616C7565320000

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

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200690x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)  
Tag: Unique Batch Item ID (0x4200990x420093), Type: Octet String (0x08), Data: 42C6D3ED5BFE4F34BA3EA60548ECB699  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1  
Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)  
Tag: Unique Batch Item ID (0x4200990x420093), Type: Octet String (0x08), Data: a391110F7716FCFB321984E716274A3D  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2  
Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2

420075010000017042007401000000384200670100000020420068020000004000000010000000042006902000000040  
000000000000042000D020000000400000002000000042000F010000009042005A0500000040000000E0000000042  
0090080000000842C6D3ED5BFE4F344200760100000068420091070000002437666261303834392D613363322D3464386  
32D383164642D3961313939393437653437640000000420008010000003042000A070000000C782D6174747269627574  
65310000000042000B070000000E4D6F64696669656456616C756531000042000F010000009042005A05000000400000  
00E00000000420090800000008A391110F7716FCFB4200760100000068420091070000002437666261303834392D6133  
63322D346438632D383164642D3961313939393437653437640000000420008010000003042000A070000000C782D617  
47472696275746532000000042000B070000000E4D6F64696669656456616C7565320000

42007801000001704200770100000038420069010000002042006A0200000004000000010000000042006B02000000040  
000000000000042000D020000000400000002000000042000F010000009042005C0500000040000000E0000000042  
00930800000008BA3EA60548ECB6994200790100000068420094070000002430613333653833652D356237612D3438363  
52D393634612D38643163336266396165330000000420008010000003042000A070000000C782D6174747269627574  
65310000000042000B070000000E4D6F64696669656456616C756531000042000F010000009042005C05000000400000  
00E00000000420093080000008321984E716274A3D4200790100000068420094070000002430613333653833652D3562  
37612D343836352D393634612D38643163336266396165330000000420008010000003042000A070000000C782D617  
47472696275746532000000042000B070000000E4D6F64696669656456616C7565320000

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



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

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC07326 (Mon Sep 28 0x000000004AFBED26 (Thu Nov 12 12:10:26+14 CEST30 CET 2009)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)  
Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: 42C6D3ED5BFE4F34BA3EA60548ECB699  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1  
Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)  
Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: A391110F7716FCFD321984E716274A3D  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2  
Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2

42007801000001A0420077010000004842006701000000204200680200000040000000100000004200690200000040  
000000000000042008F090000000000000004AC0732642000D02000000400000002000000042000F01000000A042  
005A05000000040000000E00000000420090080000000842C6D3ED5BFE4F3442007C05000000040000000000000420  
0790100000068420091070000002437666261303834392D613363322D346438632D383164642D39613139393934376534  
3764000000042008010000003042000A070000000C782D61747472696275746531000000042000B070000000E4D6F6  
4696669656456616C756531000042000F01000000A042005A0500000040000000E00000000420090080000008A39111  
0F7716FCFD42007C0500000004000000000000004200790100000068420091070000002437666261303834392D61336  
3322D346438632D383164642D396131393939343765343764000000042008010000003042000A070000000C782D6174  
7472696275746532000000042000B070000000E4D6F64696669656456616C756532000042007B01000001A042007A010  
0000048420069010000002042006A020000000400000001000000042006B020000004000000000000004200920900  
000008000000004AFBED2642000D020000000400000002000000042000F01000000A042005C05000000040000000E0000  
000004200930800000008BA3EA60548ECB69942007F05000000040000000000000042007C0100000068420094070000  
002430613333653833652D356237612D343836352D393634612D386431633362663961653300000004200080100000  
03042000A070000000C782D61747472696275746531000000042000B070000000E4D6F64696669656456616C75653100  
0042000F01000000A042005C0500000040000000E00000000420093080000008321984E716274A3D42007F050000000  
40000000000000042007C0100000068420094070000002430613333653833652D356237612D343836352D393634612D  
38643163336266396165330000000420008010000003042000A070000000C782D6174747269627574653200000004  
2000B070000000E4D6F64696669656456616C7565320000

7 Client B:  
Delete attribute [batch]

In: uuidKey, attributeNames={x-attribute1}

In: uuidKey, attributeNames={x-attribute2}

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)

Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: FB10B7D6A5F8F02FD5C6DF842DAEECD8

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)

Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: 3B5C2DE222A01A87572D4F0D433DAB10

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

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

42007501000001304200740100000003842006701000000204200680200000004000000010000000420069020000000400000000000042000D020000000400000002000000042000F010000007042005A0500000040000000F0000000042000760100000048420091070000002437666261303834392D613363322D346438632D383164642D396131393939343765343764000000042000A070000000C782D61747472696275746531000000042000F010000007042005A0500000040000000F000000004200908000000083B5C2DE222A01A874200760100000048420091070000002437666261303834392D613363322D346438632D383164642D396131393939343765343764000000042000A070000000C782D6174747269627574653200000000

420078010000013042007701000000038420069010000002042006A020000000400000001000000042006B0200000004000000000000042000D020000000400000002000000042000F010000007042005C0500000040000000F0000000042000760100000048420091070000002430613333653833652D356237612D343836352D393634612D3864316333626639616533000000042000A070000000C782D61747472696275746531000000042000F010000007042005C0500000040000000F00000000420093080000008572D4F0D433DAB104200790100000048420091070000002430613333653833652D356237612D343836352D393634612D3864316333626639616533000000042000A070000000C782D6174747269627574653200000000

Out: uuidKey, attributeNames={x-attribute1}

Out: uuidKey, attributeNames={x-attribute2}

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:

Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC07327 (Mon-Sep

```

28-0x000000004AFBED26 (Thu Nov 12 12:10:26-15 CEST30 CET 2009)
  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
    Tag: Unique Batch Item ID (0x420090x420093), Type: Octet String (0x08), Data:
      FB10B7D6A5F8F02FD5C6DF842DAEED8
    Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
    Tag: Attribute (0x420008), Type: Structure (0x01), Data:
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
      Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1
    Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
      Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
      Tag: Unique Batch Item ID (0x420090x420093), Type: Octet String (0x08), Data:
        3B5C2DE222A01A87572D4F0D433DAB10
      Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
      Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:
        Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2

420078010000001A0420077010000004842006701000000204200680200000004000000010000000042006902000000040
0000000000000042008F09000000000000004AC0732742000D020000000400000002000000042000F01000000A042
005A05000000040000000F00000004200900800000008FB10B7D6A5F8F02FD5C6DF842DAEED8
0790100000068420091070000002437666261303834392D61336332D346438632D383164642D39613139393934376534
3764000000042008010000003042000A070000000E782D61747472696275746531000000042000B070000000E4D6F6
469669656456616C756531000042000F01000000A042005A05000000040000000F0000000042009008000000083B5C2D
E222A01A8742007C0500000004000000000000004200790100000068420091070000002437666261303834392D61336
3322D346438632D383164642D396131393939343765343764000000042008010000003042000A070000000E782D6174
7472696275746532000000042000B070000000E4D6F64696669656456616C756532000042007B01000001A042007A010
0000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900
00008000000004AFBED264200D02000000040000002000000042000F01000000A042005C05000000040000000F000
0000420093080000008D5C6DF842DAEED842007F05000000040000000000000042007C0100000068420094070000
002430613333653833652D37612D343836352D393634612D3864316333626639616533000000042000801000000
03042000A070000000E782D617474726962757465310000000042000B070000000E4D6F64696669656456616C75653100
0042000F01000000A042005C05000000040000000F00000000420093080000008572D4F0D433DAB1042007F050000000
40000000000000042007C0100000068420094070000002430613333653833652D356237612D343836352D393634612D
38643163336266396165330000000420008010000003042000A070000000E782D6174747269627574653200000004
2000B070000000E4D6F64696669656456616C7565320000

```

```

8 Client A:
  Destroy (symmetric key)
  In: uuidKey

  Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

```

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: [7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3](#)

[42007501000000904200740100000038420067010000002042006802000000040000000100000000420069020000000400000000000042000D0200000004000000010000000042000F010000004842005A050000000400000014000000004200760100000030420091070000002437666261303834392D613363322D346438632D383164642D39613139393934376534376400000000](#)

[42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961653300000000](#)

**Out: uuidKey**

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:

Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: ~~0x00000004AC07327 (Mon Sep 28 0x00000004AFBED27 (Thu Nov 12 12:10:26+15 CEST 2009))~~

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

Tag: Result Status (0x4200760x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: [7fba0849-a3e2-4d8e-81dd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3](#)

[42007801000000B04200770100000048420067010000002042006802000000040000000100000000420069020000000400000000000042000D0200000000420008F0900000008000000004AC0732742000D0200000004000000010000000042000F010000005842005A0500000004000000014000000004200760100000030420091070000002437666261303834392D613363322D346438632D383164642D3961313939393437653437640000000042007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000000420092090000008000000004AFBED2742000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F05000000040000000000000042007C0100000030420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961653300000000](#)

9

**Client A:**

**Get (symmetric key)**

**In: uuidKey**

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: [7fba0849-a3e2-4d8e-8idd-9a199947e47d0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3](#)

[42007501000000090420074010000003842006701000000204200680200000004000000010000000420069020000000400000000000042000D0200000004000000010000000042000F010000004842005A05000000040000000A0000000042007601000000030420091070000002437666261303834392D613363322D346438632D383164642D39613139393934376534376400000000](#)

[420078010000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A0000000042007901000000030420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961653300000000](#)

**Out: Operation Failed, Item Not Found**

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:

Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: ~~0x000000004AC07327 (Mon Sep 28 0x000000004AFBED27 (Thu Nov 12 12:10:26-15 CEST31 CET 2009)~~

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)

Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000001 ([Operation Failed](#))

Tag: Result Reason (0x42007B0x42007E), Type: Enumeration (0x05), Data: 0x00000001 (Item Not Found)

Tag: Result Message (0x42007A0x42007D), Type: Text String (0x07), Data: [No Cryptographic Object found with given Unique Identifierdoes not exist](#)

[420078010000000D04200770100000048420067010000002042006802000000040000000100000004200690200000004000000000000420008F0900000008000000004AC0732742000D020000000400000001000000042000F010000007842005A05000000040000000A0000000042007C0500000004000000010000000042007B0500000004000000010000000042007A070000003A4E6F2043727970746F67726170686963204F626A65637420666F756E64207769746820676976656E20556E69717565204964656E7469666965720000000000042007B01000000A842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2742000D0200000004000000010000000042000F010000005042005C05000000040000000A0000000042007F0500000004000000001000000042007E0500000004000000010000000042007D0700000154F626A65637420646F6573206E6F74206578697374000000](#)

10 Client A:  
 Destroy (template)  
 In: uuidTemplate

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

	<p>Tag: Request Payload (<a href="#">0x4200760x420079</a>), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (<a href="#">0x4200910x420094</a>), Type: Text String (0x07), Data: <a href="#">8383198b-4600-4388-955f-2802ee699e9e45d8629a-9ad1-41b3-9d09-941f2a595da3</a></p> <p><a href="#">4200750100000090420074010000003842006701000000204200680200000004000000010000000042006902000000040000000000000042000D0200000004000000010000000042000F010000004842005A0500000004000000014000000004200760100000030420091070000002438333833313938622B343630302D343338382B393535662D323830326336393965396300000000</a></p> <p><a href="#">42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000014000000004200790100000030420094070000002434356438363239612D396164312D343162332D396430392D39343166326135393564613300000000</a></p> <p><b>Out: uuidTemplate</b></p> <p>Tag: Response Message (<a href="#">0x4200780x42007B</a>), Type: Structure (0x01), Data:</p> <p>Tag: Response Header (<a href="#">0x4200770x42007A</a>), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (<a href="#">0x4200670x420069</a>), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (<a href="#">0x4200680x42006A</a>), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (<a href="#">0x4200690x42006B</a>), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Time Stamp (<a href="#">0x42008F0x420092</a>), Type: Date-Time (0x09), Data: <a href="#">0x000000004AC07327 (Mon Sep 28 0x000000004AFBED27 (Thu Nov 12 12:10:26-15 CEST31 CET 2009)</a></p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (<a href="#">0x42005A0x42005C</a>), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</p> <p>Tag: Result Status (<a href="#">0x4200760x42007F</a>), Type: Enumeration (0x05), Data: 0x00000000 (Success)</p> <p>Tag: Response Payload (<a href="#">0x4200790x42007C</a>), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (<a href="#">0x4200910x420094</a>), Type: Text String (0x07), Data: <a href="#">8383198b-4600-4388-955f-2802ee699e9e45d8629a-9ad1-41b3-9d09-941f2a595da3</a></p> <p><a href="#">4200780100000090420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042000F0900000008000000004AC0732742000D0200000004000000010000000042000F010000005842005A05000000040000000140000000042007C0500000004000000000000004200790100000030420091070000002438333833313938622B343630302D343338382B393535662D32383032633639396539630000000042007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000000042000D2090000008000000004AFBED2742000D0200000004000000010000000042000F010000005842005C05000000040000000140000000042007F05000000040000000000000042007C0100000030420094070000002434356438363239612D396164312D343162332D396430392D39343166326135393564613300000000</a></p>
11	<p><b>Client A:</b></p> <p><b>Get (template)</b></p> <p><b>In: uuidTemplate</b></p> <p>Tag: Request Message (<a href="#">0x4200750x420078</a>), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (<a href="#">0x4200740x420077</a>), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (<a href="#">0x4200670x420069</a>), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (<a href="#">0x4200680x42006A</a>), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (<a href="#">0x4200690x42006B</a>), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (<a href="#">0x42005A0x42005C</a>), Type: Enumeration (0x05), Data: 0x0000000A (Get)</p> <p>Tag: Request Payload (<a href="#">0x4200760x420079</a>), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (<a href="#">0x4200910x420094</a>), Type: Text String (0x07), Data: <a href="#">8383198b-4600-4388-955f-2802ee699e9e45d8629a-9ad1-41b3-9d09-941f2a595da3</a></p>

42007501000000904200740100000038420067010000002042006802000000400000001000000004200690200000040  
0000000000000042000D0200000004000000010000000042000F010000004842005A05000000040000000A0000000042  
00760100000030420091070000002438333833313938622D343630302D343338382D393535662D3238303263633639396  
5396300000000

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000040  
0000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A0000000042  
00790100000030420094070000002434356438363239612D396164312D343162332D396430392D3934316632613539356  
4613300000000

Out: Operation Failed, Item Not Found

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC07327 (Mon Sep 28 0x000000004AFBED27 (Thu Nov 12 12:10:26+15 cEST 2009))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Failed)  
Tag: Result Reason (0x42007B0x42007E), Type: Enumeration (0x05), Data: 0x00000001 (Item Not Found)  
Tag: Result Message (0x42007A0x42007D), Type: Text String (0x07), Data: No Cryptographic Object found with given Unique Identifier

42007801000000D04200770100000048420067010000002042006802000000400000001000000004200690200000040  
0000000000000042008F0900000008000000004AC0732742000D020000004000000010000000042000F010000007842  
005A05000000040000000A0000000042007C0500000004000000010000000042007B05000000040000000100000000420  
07A070000003A4E6F2043727970746F67726170686963204F626A65637420666F756E64207769746820676976656E2055  
6E69717565204964656E74696669657200000000000042007B01000000D042007A0100000048420069010000002042006  
A0200000004000000010000000042006B020000000400000000000000004200920900000008000000004AFBED2742000D  
0200000004000000010000000042000F010000007842005C05000000040000000A0000000042007F05000000040000000  
10000000042007E0500000004000000010000000042007D070000003A4E6F2043727970746F67726170686963204F626A  
65637420666F756E64207769746820676976656E20556E69717565204964656E746966696572000000000000

87

88 [3.1.5 Use-case: Register / Destroy Secret Data](#)

89 [In this use-case the client issues a Register request containing a Secret Data object, whereby the server](#)  
90 [registers the object and returns the Unique Identifier. To clean up, the client then performs a Destroy](#)  
91 [operation to destroy the object.](#)

92

Time	Request/Response messages
0	<a href="#">Register (secret data)</a> <a href="#">In: objectType='0000007' (Secret Data), attributes={ CryptographicUsageMask='0000002' }</a>  Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

	<p> <a href="#">Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</a>  <a href="#">Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</a>  <a href="#">Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</a>  <a href="#">Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)</a>  <a href="#">Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000007 (Secret Data)</a>  <a href="#">Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Attribute (0x420008), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: <u>Cryptographic Usage Mask</u></a>  <a href="#">Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000002 (Verify)</a>  <a href="#">Tag: Secret Data (0x420085), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Secret Data Type (0x420086), Type: Enumeration (0x05), Data: 0x00000001</a>  <a href="#">Tag: Key Block (0x420040), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000002</a>  <a href="#">Tag: Key Value (0x420045), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Key Material (0x420043), Type: Octet String (0x08), Data: <u>53656372657450617373776F7264</u></a>   42007801000001004200770100000038420069010000002042006A0200000004000000010000000042006B0200000004  00000000000000042000D0200000004000000010000000042000F01000000B842005C05000000040000000300000000  4200790100000A0420057050000000400000007000000004200910100000038420008010000003042000A0700000018  43727970746F67726170686963205573616765204D61736B42000B020000000400000002000000004200850100000048  42008605000000400000001000000004200400100000030420042050000000400000002000000004200450100000018  42004308000000E53656372657450617373776F72640000 </p> <p><b>Out: uuidObject</b></p> <p> <a href="#">Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</a>  <a href="#">Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</a>  <a href="#">Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B7924D1 (Mon Feb 15 11:41:21 CET 2010)</a>  <a href="#">Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</a>  <a href="#">Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)</a>  <a href="#">Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</a>  <a href="#">Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: <u>39622cc2-e5d4-4da9-9f10-3bdf64b0e760</u></a>   42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004  0000000000000004200920900000008000000004B7924D142000D0200000004000000010000000042000F0100000058  42005C0500000004000000030000000042007F05000000040000000000000042007C01000000304200940700000024  33393632326363322D653564342D346461392D396631302D33626466363462306537363000000000 </p>
1	<p><b>Destroy (secret data)</b></p> <p><b>In: uuidObject</b></p>



```

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
    Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 39622cc2-e5d4-4da9-
9f10-3bdf64b0e760

42007801000000904200770100000038420069010000002042006A020000004000000010000000042006B0200000004
000000000000000042000D02000000400000001000000042000F010000004842005C05000000040000001400000000
4200790100000030420094070000002433393632326363322D653564342D346461392D396631302D3362646636346230
6537363000000000

Out: uuidKey

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

42007B01000000B042007A0100000048420069010000002042006A020000004000000010000000042006B0200000004
000000000000004200920900000008000000004B7924D142000D020000004000000010000000042000F0100000058
42005C0500000004000000140000000042007F050000000400000000000000042007C01000000304200940700000024
33393632326363322D653564342D346461392D396631302D33626466363462306537363000000000

```

93  
94

95 **3.23.2 Use-case: Asynchronous Locate**

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

102  
103 This use-case shows the use of two clients with the same assumptions as in the use-case described in  
104 Section 3.1.4 Since the client is unable to force the server to respond asynchronously, it is possible for a

Formatted: Indent: Left: 0 pt, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 36 pt + Indent at: 36 pt, Don't adjust space between Latin and Asian text  
Formatted: Font: Not Bold

105 server to respond synchronously to the requests issued at times 1 and 4, in which case the expected  
 106 response are the ones shown at times 2 and 5, respectively. In the case of the server not responding  
 107 asynchronously to the Locate requests, the client is permitted to skip the requests illustrated at time 7 and  
 108 8.  
 109

Time	Client A
0	<p>Client A:            Create (symmetric key)            In: objectType = '00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128',            Name={ NameValue='Key1', NameType='00000001' }, CryptographicUsageMask='00000004',            ObjectGroup='Group1' }</p> <p>Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:            Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:            Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:            Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)            Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)            Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)            Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:            Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)            Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:            Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric            Key)            Tag: Template-Attribute (0x42008E0x420091), 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 (0x4200530x420055), Type: Text String (0x07), Data: Key1            Tag: Name Type (0x4200520x420054), Type: Enumeration (0x05), Data: 0x00000001            (Uninterpreted text string)            Tag: Attribute (0x420008), Type: Structure (0x01), Data:            Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage            Mask            Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt)            Tag: Attribute (0x420008), Type: Structure (0x01), Data:            Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group            Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1</p> <p>420075010000019042007401000000384200670100000020420068020000000400000001000000042006902000000040            000000000000042000B020000000400000001000000042000F010000014842005A050000000400000001000000042            00760100000130420055050000000400000002000000042008E010000011842008010000003042000A0700000017437            27970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200            0A070000001443727970746F6772617068696320416C656E677468000000042000B0200000004000000080000000042000            8010000003842000A07000000044E616D65000000042000B010000002042005307000000044B6579310000000420052            0500000004000000010000000420008010000003042000A070000001843727970746F677261706869632055736167652</p>

04D61736B42000B0200000004000000040000000420008010000002842000A070000000C4F626A6563742047726F7570  
0000000042000B070000000647726F7570310000  
42007801000001904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040  
0000000000000042000D020000000400000001000000042000F010000014842005C0500000004000000010000000042  
00790100000130420057050000000400000002000000004200910100000118420008010000003042000A0700000017437  
27970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200  
0A070000001443727970746F67726170686963204C656E677468000000042000B02000000040000000800000000042000  
8010000003842000A07000000044E616D65000000042000B010000002042005507000000044B65793100000000420054  
05000000040000000100000000420008010000003042000A0700000001843727970746F677261706869632055736167652  
04D61736B42000B0200000004000000040000000420008010000002842000A070000000C4F626A6563742047726F7570  
0000000042000B070000000647726F7570310000

Out: objectType = '00000002', uuidKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0781B (Mon Sep 28 0x000000004AFBED28 (Thu Nov 12 12:10:47+23 CEST 2009))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 8b961211-97e7-40a6-8664-ed33491dab5e95a0e6b3-8edc-4ffb-a88e-e164539dbcca

420078010000000C04200770100000004842006701000000204200680200000004000000010000000042006902000000040  
0000000000000042008F0900000008000000004AC0781B42000D0200000004000000010000000042000F010000006842  
005A0500000004000000010000000042007C05000000040000000000000042007901000000404200550500000004000  
000020000000042009107000000024386239363132331312D393763372D343061362D383636342D65643333343931646162  
3563000000042007B010000000C042007A01000000048420069010000002042006A0200000004000000010000000042006  
B0200000040000000000000004200920900000008000000004AFBED2842000D0200000004000000010000000042000F  
010000006842005C0500000004000000010000000042007F050000000400000000000000042007C010000000404200570  
50000000400000002000000004200940700000002439356130653662332D386564632D346666622D613838652D65313634  
3533396462636100000000

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

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

Tag: Request Payload (0x4200760x420079), 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 (0x4200530x420055), Type: Text String (0x07), Data: Key1  
Tag: Name Type (0x4200520x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

4200750100000000E04200740100000048420067010000002042006802000000040000000100000000420069020000000400000000000000420007060000000800000000000000000000142000D0200000004000000010000000042000F010000008842005A050000000400000008000000004200760100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000020000000420008010000003842000A07000000044E616D65000000042000B010000002042005307000000044B6579310000000042005205000000040000000100000000

420078010000000E04200770100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200070600000080000000000000000142000D0200000004000000010000000042000F010000008842005C050000000400000008000000004200790100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000020000000420008010000003842000A07000000044E616D65000000042000B010000002042005507000000044B6579310000000042005405000000040000000100000000

Out: asyncCorrValue1

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC0781C (Mon Sep 28 0x000000004AFBED28 (Thu Nov 12 12:10:47:24 CEST32 CET 2009))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Pending)  
Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: D1DE142AC6367B4B130BC369AF005A7F

420078010000008842007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000004200070600000080000000000000000142000D0200000004000000010000000042000F010000003042005A0500000004000000080000000042007C05000000040000000200000004200060800000008D1DE142AC6367B4B42007B010000008842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2842000D0200000004000000010000000042000F010000003042005C0500000004000000080000000042007F0500000004000000020000000420006080000008130BC369AF005A7F

2 Client B:  
Poll\*  
In: asyncCorrValue1

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor ([0x4200690x42006B](#)), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation ([0x42005A0x42005C](#)), Type: Enumeration (0x05), Data: 0x0000001A (Poll)

Tag: Request Payload ([0x4200760x420079](#)), Type: Structure (0x01), Data:

Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: [D1DE142AC6367B4B130BC369AF005A7F](#)

[42007501000000704200740100000038420067010000002042006802000000400000001000000042006902000000400000000000042000D02000000400000001000000042000F010000002842005A0500000040000001A00000000420076010000001042000608000000008D1DE142AC6367B4B](#)

[42007801000000704200770100000038420069010000002042006A02000000400000001000000042006B020000004000000000000042000D02000000400000001000000042000F010000002842005C0500000040000001A0000000042007901000000104200060800000008130BC369AF005A7F](#)

**Out: uuidKey1**

Tag: Response Message ([0x4200780x42007B](#)), Type: Structure (0x01), Data:

Tag: Response Header ([0x4200770x42007A](#)), Type: Structure (0x01), Data:

Tag: Protocol Version ([0x4200670x420069](#)), Type: Structure (0x01), Data:

Tag: Protocol Version Major ([0x4200690x42006A](#)), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor ([0x4200690x42006B](#)), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp ([0x42008F0x420092](#)), Type: Date-Time (0x09), Data: ~~0x00000004AC0781C (Mon Sep 28 0x000000004AFBED28 (Thu Nov 12 12:10:47+24 CEST 2009)~~

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

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

Tag: Operation ([0x42005A0x42005C](#)), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

Tag: Result Status ([0x42007E0x42007F](#)), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload ([0x4200790x42007C](#)), Type: Structure (0x01), Data:

Tag: Unique Identifier ([0x4200910x420094](#)), Type: Text String (0x07), Data: ~~8b961211-97e7-40a6-8664-ed33491dab5e95a0e6b3-8edc-4ffb-a88e-e164539dbcca~~

[42007801000000B04200770100000048420067010000002042006802000000400000001000000042006902000000400000000000042000D02000000400000001000000042000F0100000005842005A05000000400000008000000042007C05000000400000000000004200790100000030420091070000002438623936313231312D393763372D343061362D383636342D656433333439316461623563000000042007B01000000B042007A0100000048420069010000002042006A02000000400000001000000042006B02000000400000000000000042009209000000800000004AFBED284200D02000000400000001000000042000F010000005842005C05000000400000008000000042007F050000004000000000000042007C0100000030420094070000002439356130653662332D386564632D34666622D613838652D65313634353339646263636100000000](#)

3 Client B:

Get (symmetric key)

In: uuidKey1

Tag: Request Message ([0x4200750x420078](#)), Type: Structure (0x01), Data:

Tag: Request Header ([0x4200740x420077](#)), Type: Structure (0x01), Data:

Tag: Protocol Version ([0x4200670x420069](#)), Type: Structure (0x01), Data:

Tag: Protocol Version Major ([0x4200690x42006A](#)), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor ([0x4200690x42006B](#)), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation ([0x42005A0x42005C](#)), Type: Enumeration (0x05), Data: 0x0000000A (Get)

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 8b961211-97e7-40a6-8664-ed33491dab5e95a0e6b3-8edc-4ffb-a88e-e164539dbcca  
  
4200750100000090420074010000003842006701000000204200680200000040000000100000004200690200000040  
000000000000042000D02000000400000001000000042000F010000004842005A0500000040000000A0000000042  
00760100000030420091070000002438623936313231312D393763372D343061362D383636342D656433334393164616  
2356200000000  
  
42007801000000904200770100000038420069010000002042006A02000000400000001000000042006B0200000040  
000000000000042000D02000000400000001000000042000F010000004842005C0500000040000000A0000000042  
00790100000030420094070000002439356130653662332D386564632D346666622D613838652D6531363435333964626  
3636100000000

Out: objectType = '0000002', uuidKey1, symmetricKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0781D (Mon Sep 28 0x000000004AFBED29 (Thu Nov 12 12:10:47:25 CEST33 CET 2009))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 8b961211-97e7-40a6-8664-ed33491dab5e95a0e6b3-8edc-4ffb-a88e-e164539dbcca  
Tag: Symmetric Key (0x42008C0x42008F), Type: Structure (0x01), Data:  
Tag: Key Block (0x42003E0x420040), Type: Structure (0x01), Data:  
Tag: Key Format Type (0x4200490x420042), Type: Enumeration (0x05), Data: 0x00000001  
Tag: Key Value (0x4200430x420045), Type: Structure (0x01), Data:  
Tag: Key Material (0x4200410x420043), Type: Octet String (0x08), Data: A1DF7B733D8DF7056623FE2D880EF62C42002605000000400000003000000004200280200000040000000  
A1DF7B733D8DF7056623FE2D880EF62C42002605000000400000003000000004200280200000040000000  
Tag: Cryptographic Algorithm (0x4200260x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)  
Tag: Cryptographic Length (0x4200280x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

4200780100000120420077010000004842006701000000204200680200000040000000100000004200690200000040  
000000000000042008F09000000000000004AC0781D42000D02000000400000001000000042000F01000000C842  
005A0500000040000000A000000042007C0500000040000000000000042007901000000A0420055050000004000  
000020000000420091070000002438623936313231312D393763372D343061362D383636342D6564333343931646162  
3563000000042008C010000005842003E0100000050420040050000004000000010000000420043010000001842004  
1000000010A1DF7B733D8DF7056623FE2D880EF62C42002605000000400000003000000004200280200000040000000  
8000000042007B010000012042007A0100000048420069010000002042006A02000000400000001000000042006B0  
200000040000000000000420092090000008000000004AFBED2942000D02000000400000001000000042000F01  
000000C842005C0500000040000000A000000042007F05000000040000000000000042007C01000000A0420057050  
0000040000000200000000420094070000002439356130653662332D386564632D346666622D613838652D6531363435  
33396462636361000000042008F0100000058420040010000005042004205000000400000001000000042004501000  
000184200430800000010BEF01F82DFB4682A01C2A08413834AAB42002805000000400000003000000042002A020000  
0004000000800000000

4 Client B:

Locate (symmetric key by group)

In: asynchronousIndicator='TRUE', attributes={ objectType = '0000002', ObjectGroup='Group1' }

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type  
Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group  
Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1

420075010000000042007401000000484200670100000020420068020000004000000010000000420069020000004000000000004200070600000008000000000000000142000D02000000400000001000000042000F010000007842005A05000000400000008000000000004200760100000060420008010000002842000A070000000B4F626A65637420547970650000000042000B050000004000000020000000420008010000002842000A070000000C4F626A6563742047726F7570000000042000B070000000647726F7570310000

42007801000000004200770100000048420069010000002042006A02000000400000001000000042006B0200000040000000000042000706000000800000000000000142000D02000000400000001000000042000F010000007842005A05000000400000008000000000004200790100000060420008010000002842000A070000000B4F626A65637420547970650000000042000B050000004000000020000000420008010000002842000A070000000C4F626A6563742047726F7570000000042000B070000000647726F7570310000

Out: asyncCorrValue2

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0781D (Mon Sep 28 0x000000004AFBED29 (Thu Nov 12 12:10:47+25 CEST 2009))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Pending)  
Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 2BCF4F694617FC3048D43C207CD1FB3A

42007801000000088420077010000004842006701000000204200680200000040000000100000004200690200000040000000000042000F0100000003042005A050000004000000080000000000042007C0500000040000000200000004200060800000082BCF4F694617FC3042007B010000008842007A0100000048420069010000002042006A02000000400000001000000042006B020000004000000000004200092090000008000000004AFBED2942000D02000000400000001000000042000F010000003042005

	<a href="#">C0500000004000000080000000042007F0500000004000000020000000042006080000000848D43C207CD1FB3A</a>
5	<p>Client B: Poll* In: asyncCorrValue2</p> <p>Tag: Request Message (<a href="#">0x4200750x420078</a>), Type: Structure (0x01), Data:      Tag: Request Header (<a href="#">0x4200740x420077</a>), Type: Structure (0x01), Data:      Tag: Protocol Version (<a href="#">0x4200670x420069</a>), Type: Structure (0x01), Data:        Tag: Protocol Version Major (<a href="#">0x4200680x42006A</a>), Type: Integer (0x02), Data: 0x00000001 (1)        Tag: Protocol Version Minor (<a href="#">0x4200690x42006B</a>), Type: Integer (0x02), Data: 0x00000000 (0)        Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)        Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:          Tag: Operation (<a href="#">0x42005A0x42005C</a>), Type: Enumeration (0x05), Data: 0x0000001A (Poll)          Tag: Request Payload (<a href="#">0x4200760x420079</a>), Type: Structure (0x01), Data:            Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:            <a href="#">2DCF4F694617FC3048D43C207CD1FB3A</a></p> <p><a href="#">42007501000000704200740100000038420067010000002042006802000000040000000100000000420069020000000400000000000042000D0200000004000000010000000042000F010000002842005A0500000040000001A0000000042007601000000104200608000000082DCF4F694617FC30</a></p> <p><a href="#">42007801000000704200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000002842005C0500000040000001A00000000420079010000001042006080000000848D43C207CD1FB3A</a></p> <p>Out: uuidKey2</p> <p>Tag: Response Message (<a href="#">0x4200780x42007B</a>), Type: Structure (0x01), Data:      Tag: Response Header (<a href="#">0x4200770x42007A</a>), Type: Structure (0x01), Data:      Tag: Protocol Version (<a href="#">0x4200670x420069</a>), Type: Structure (0x01), Data:        Tag: Protocol Version Major (<a href="#">0x4200680x42006A</a>), Type: Integer (0x02), Data: 0x00000001 (1)        Tag: Protocol Version Minor (<a href="#">0x4200690x42006B</a>), Type: Integer (0x02), Data: 0x00000000 (0)        Tag: Time Stamp (<a href="#">0x42008F0x420092</a>), Type: Date-Time (0x09), Data: <a href="#">0x000000004AC0781D (Mon Sep 28 0x000000004AFBED29 (Thu Nov 12 12:10:47-25 CEST33 CET 2009)</a>        Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)        Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:          Tag: Operation (<a href="#">0x42005A0x42005C</a>), Type: Enumeration (0x05), Data: 0x00000008 (Locate)          Tag: Result Status (<a href="#">0x42007C0x42007F</a>), Type: Enumeration (0x05), Data: 0x00000000 (Success)          Tag: Response Payload (<a href="#">0x4200790x42007C</a>), Type: Structure (0x01), Data:            Tag: Unique Identifier (<a href="#">0x4200910x420094</a>), Type: Text String (0x07), Data: <a href="#">8b961211-97e7-40a6-8664-ed33491dab5e95a0e6b3-8edc-4ffb-a88e-e164539dbcca</a></p> <p><a href="#">42007801000000B04200770100000048420067010000002042006802000000040000000100000000420069020000000400000000000042000D0200000004000000010000000042000F010000002842005A0500000040000001A0000000042007601000000104200608000000084AC0781D42000D0200000004000000010000000042000F010000002842005C0500000040000001A00000000420079010000001042006080000000848D43C207CD1FB3A</a></p>
6	<p>Client B: Get (symmetric key)</p>



In: uuidKey2

Tag: Request Message ([0x4200750x420078](#)), Type: Structure (0x01), Data:

Tag: Request Header ([0x4200740x420077](#)), Type: Structure (0x01), Data:

Tag: Protocol Version ([0x4200670x420069](#)), Type: Structure (0x01), Data:

Tag: Protocol Version Major ([0x4200680x42006A](#)), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor ([0x4200690x42006B](#)), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation ([0x42005A0x42005C](#)), Type: Enumeration (0x05), Data: 0x0000000A (Get)

Tag: Request Payload ([0x4200760x420079](#)), Type: Structure (0x01), Data:

Tag: Unique Identifier ([0x4200910x420094](#)), Type: Text String (0x07), Data: [8b961211-97e7-40a6-8664-ed33491dab5e95a0e6b3-8edc-4ffb-a88e-e164539dbcca](#)

[4200750100000090420074010000003842006701000000204200680200000040000000100000004200690200000040000000000042000D020000004000000010000000042000F010000004842005A0500000040000000A00000004200760100000030420091070000002438623936313231312D393763372D343061362D383636342D65643333343931646162356200000000](#)

[42007801000000904200770100000038420069010000002042006A02000000400000001000000042006B02000000400000000000042000D020000004000000010000000042000F010000004842005C0500000040000000A00000004200790100000030420094070000002439356130653662332D386564632D346666622D613838652D65313634353339646263636100000000](#)

Out: objectType = '00000002', uuidKey2, symmetricKey

Tag: Response Message ([0x4200780x42007B](#)), Type: Structure (0x01), Data:

Tag: Response Header ([0x4200770x42007A](#)), Type: Structure (0x01), Data:

Tag: Protocol Version ([0x4200670x420069](#)), Type: Structure (0x01), Data:

Tag: Protocol Version Major ([0x4200680x42006A](#)), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor ([0x4200690x42006B](#)), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp ([0x42008F0x420092](#)), Type: Date-Time (0x09), Data: [0x00000004AC0781D \(Mon Sep 28 0x00000004AFBED29 \(Thu Nov 12 12:10:47:25 CEST33 CET 2009\)](#)

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

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

Tag: Operation ([0x42005A0x42005C](#)), Type: Enumeration (0x05), Data: 0x0000000A (Get)

Tag: Result Status ([0x4200760x42007F](#)), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload ([0x4200790x42007C](#)), Type: Structure (0x01), Data:

Tag: Object Type ([0x4200550x420057](#)), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier ([0x4200910x420094](#)), Type: Text String (0x07), Data: [8b961211-97e7-40a6-8664-ed33491dab5e95a0e6b3-8edc-4ffb-a88e-e164539dbcca](#)

Tag: Symmetric Key ([0x42008C0x42008F](#)), Type: Structure (0x01), Data:

Tag: Key Block ([0x42003E0x420040](#)), Type: Structure (0x01), Data:

Tag: Key Format Type ([0x4200490x420042](#)), Type: Enumeration (0x05), Data: 0x00000001

Tag: Key Value ([0x4200430x420045](#)), Type: Structure (0x01), Data:

Tag: Key Material ([0x4200410x420043](#)), Type: Octet String (0x08), Data: [A1DF7B733D8DF7056623FE2D880EF62CBEF01F82DFB4682A01C2A08413834AAB](#)

Tag: Cryptographic Algorithm ([0x4200260x420028](#)), Type: Enumeration (0x05), Data: 0x00000003 (AES)

Tag: Cryptographic Length ([0x4200280x42002A](#)), Type: Integer (0x02), Data: 0x00000080 (128)

420078010000012042007701000000484200670100000020420068020000000400000001000000004200690200000040  
000000000000042008F0900000000000000004200781D42000D0200000004000000010000000042000F0100000008842  
005A0500000004000000A0000000042007C05000000040000000000000004200790100000A0420055050000004000  
000020000000042009107000000243862393613231312D393763372D343061362D383636342D65643333343931646162  
3563000000042008C010000005842003E010000005042004005000000040000000100000000420043010000001842004  
10800000010A1DF7B733D8DF7056623FE2D880EF62C4200260500000040000000300000000420028020000004000000  
80000000042007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B0  
200000004000000000000004200920900000008000000004AFBED2942000D0200000004000000010000000042000F01  
000000C842005C0500000040000000A0000000042007F05000000040000000000000042007C01000000A0420057050  
00000040000000200000000420094070000002439356130653662332D386564632D346666622D613838652D6531363435  
33396462636361000000042008F0100000058420040010000005042004205000000400000010000000042004501000  
000184200430800000010BEF01F82DFB4682A01C2A08413834AAB420028050000004000000030000000042002A020000  
00040000008000000000

7 Client B:  
Locate (symmetric key by name)  
In: asynchronousIndicator='TRUE', attributes={ objectType = '0000002', Name= { Name='Key1', NameType='0000001' } }

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Request Payload (0x4200760x420079), 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 (0x4200530x420055), Type: Text String (0x07), Data: Key1  
Tag: Name Type (0x4200520x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007501000000E042007401000000484200670100000020420068020000000400000001000000004200690200000040  
000000000000042008F0600000000000000000000000142000D0200000004000000010000000042000F0100000008842  
005A05000000040000008000000004200760100000070420008010000002842000A070000000B4F626A6563742054797  
06500000000042000B05000000040000000200000000420008010000003842000A07000000044E616D6500000004200  
0B010000002042005307000000044B6579310000000042005205000000040000000100000000

42007801000000E04200770100000048420069010000002042006A0200000004000000010000000042006B0200000040  
000000000000042000706000000080000000000000000142000D0200000004000000010000000042000F0100000008842  
005C05000000040000008000000004200790100000070420008010000002842000A070000000B4F626A6563742054797  
06500000000042000B05000000040000000200000000420008010000003842000A07000000044E616D6500000004200  
0B010000002042005507000000044B6579310000000042005405000000040000000100000000

Out: asyncCorrValue5

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
 Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0781F (Mon Sep 28 0x000000004AFBED29 (Thu Nov 12 12:10:47:26 CEST33 CET 2009))  
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
 Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
 Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Pending)  
 Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: [D48BDD01A8FFEC804D6BBFC35FE57FBA](#)

[42007801000000884200770100000048420067010000002042006802000000040000000100000000420069020000000400000000000042008F0900000080000000004AC0781F42000D0200000004000000010000000042000F010000003042005A05000000040000000000000042007C050000000400000002000000004200660800000000D48BDD01A8FFEC8042007B010000008842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2942000D0200000004000000010000000042000F010000003042005C0500000004000000080000000042007F0500000004000000020000000042000608000000084D6BBFC35FE57FBA](#)

8 Client B:  
 Cancel  
 In: asyncCorrValue5

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
 Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
 Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
 Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000019 (Cancel)  
 Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
 Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: [D48BDD01A8FFEC804D6BBFC35FE57FBA](#)

[42007501000000704200740100000038420067010000002042006802000000040000000100000000420069020000000400000000000042000F0200000004000000010000000042000F0100000002842005A05000000040000000190000000042007601000000104200660800000000D48BDD01A8FFEC80](#)

[42007801000000704200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F0100000002842005C050000000400000001900000000420079010000001042006608000000084D6BBFC35FE57FBA](#)

Out: asyncCorrValue5, CancelResult='00000001'

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
 Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
 Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
 Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0781F (Mon Sep 28 0x000000004AFBED29 (Thu Nov 12 12:10:47:27 CEST33 CET 2009))  
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000019 (Cancel)  
Tag: Result Status (0x42007C0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: [D48BDD01A8FFEC804D6BBFC35FE57FBA](#)  
Tag: Cancellation Result (0x420012), Type: Enumeration (0x05), Data: 0x00000001 (Cancelled)

[42007801000000A04200770100000048420067010000002042006802000000400000001000000042006902000000400000000000042008F09000000800000004AC0781F42000D02000000400000001000000042000F010000004842005A05000000400000019000000042007C05000000400000000000004200790100000020420006080000008D48BDD01A8FFEC8042001205000000400000001000000042007B01000000A042007A0100000048420069010000002042006A02000000400000001000000042006B020000004000000000000042009209000000800000004AFBED294200D02000000400000001000000042000F010000004842005C05000000400000019000000042007F0500000040000000000000042007C01000000204200060800000084D6BBFC35FE57FBA420012050000004000000010000000](#)

9 Client A:  
Destroy (symmetric key)  
In: uuidKey

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: [8b961211-97e7-40a6-8664-ed32491dab5e95a0e6b3-8edc-4fffb-a88e-e164539dbcca](#)

[42007501000000904200740100000038420067010000002042006802000000400000001000000042006902000000400000000000042008F09000000800000004000000042000F010000004842005A05000000400000014000000042007601000000304200910700000024386233936313231312D393763372D343061362D383636342D65643333343931646162356300000000](#)

[42007801000000904200770100000038420069010000002042006A02000000400000001000000042006B020000004000000000000042000D02000000400000004000000042000F010000004842005C0500000040000001400000004200790100000030420094070000002439356130653662332D386564632D346666622D613838652D65313634353339646263636100000000](#)

Out: uuidKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: [0x000000004AC0781F \(Mon Sep 28 0x000000004AFBED2A \(Thu Nov 12 12:10:47:27 CEST 2009\)\)](#)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

Tag: Result Status (0x420070x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
 Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
 Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 8b961211-97e7-40a6-8664-ed33491dabb5e95a0e6b3-8edc-4ffb-a88e-e164539dbcca

4200780100000000420077010000004842006701000000204200680200000040000000100000004200690200000040  
 000000000000042008F09000000800000004AC0781F42000D0200000040000000100000004200F010000005842  
 005A05000000400000014000000042007C05000000400000000000000042007901000000304200910700000024386  
 23936313231312B393763372B343061362B383636342B65643333439316461623563000000042007B01000000B04200  
 7A0100000048420069010000002042006A020000004000000010000000042006B02000000400000000000000042009  
 2090000000800000004AFBBD2A42000D02000000400000001000000004200F010000005842005C050000004000000  
 140000000042007F05000000400000000000000042007C0100000030420094070000002439356130653662332D38656  
 4632D346666622D613838652D65313634353339646263636100000000

110 \* = executed until response is ready

111  
112

113 **44 Key life cycle support**

114

115 **4.14.1 Use-case: Revoke scenario**

116 This use-case tests the revocation aspect of the key life cycle support in KMIP. A key is created and a  
 117 Get Attribute for the State-attribute reveals that the key is in Pre-active state. The Activation Date is then  
 118 set, which changes the state to Active. The key is then revoked with a revocation reason of Compromised  
 119 and the state subsequently changed to Compromised, but this does not stop a client from being able to  
 120 add, modify and delete attributes or even get the key (since we assume here that the out-of-band  
 121 registration has been used to make the server aware of the fact that the client is capable of interpreting  
 122 the attributes of the key and determining what it is allowed to do with the key). To clean up, the created  
 123 key is finally destroyed.  
 124

Formatted: Centered

Formatted: Style Heading 1h1Level 1 Topic  
 Heading + Before: 5 pt After: 5..., Outline  
 numbered + Level: 1 + Numbering Style: 1, 2,  
 3, ... + Start at: 3 + Alignment: Left + Aligned  
 at: 0 pt + Indent at: 0 pt

Formatted: Font: Not Bold

Formatted: Indent: Left: 0 pt, Outline  
 numbered + Level: 2 + Numbering Style: 1, 2,  
 3, ... + Start at: 1 + Alignment: Left + Aligned  
 at: 36 pt + Indent at: 36 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', Name={ NameValue='Key1', NameType='00000001' }, CryptographicUsageMask='00000004' }  Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data: Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data: Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x42008E0x420091), 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 (0x4200530x420055), Type: Text String (0x07), Data: Key1  
Tag: Name Type (0x4200520x420054), 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)

42007501000001604200740100000038420067010000002042006802000000400000001000000042006902000000040  
00000000000004200000200000004000000010000000042000F010000011842005A0500000004000000010000000042  
007601000001004200550500000004000000020000000042008E01000000E8420008010000003042000A0700000017437  
27970746F6772617068696320416C676F726974686D0042000B050000000400000003000000042000801000000304200  
0A070000001443727970746F6772617068696320416C676F726974686D0042000B0500000004000000080000000042000  
8010000003842000A07000000044E616D650000000042000B010000002042005507000000044B65793100000000420052  
05000000040000000100000000420008010000003042000A070000001843727970746F677261706869632055736167652  
04D61736B42000B02000000040000000400000000

42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B02000000040  
000000000000042000B0200000004000000010000000042000F010000011842005C0500000004000000010000000042  
007901000001004200570500000004000000020000000042009101000000E8420008010000003042000A0700000017437  
27970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200  
0A070000001443727970746F6772617068696320416C676F726974686D0042000B0200000004000000080000000042000  
8010000003842000A07000000044E616D650000000042000B010000002042005507000000044B65793100000000420054  
05000000040000000100000000420008010000003042000A070000001843727970746F677261706869632055736167652  
04D61736B42000B02000000040000000400000000

Out: objectType = '00000002', uuidKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC0781F (Mon Sep 28 0x000000004AFBED2B (Thu Nov 12 12:10:47:27 CEST35 CET 2009))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333dc9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9

42007801000000042007701000000484200670100000020420068020000004000000010000000042006902000000040  
000000000000042000B0200000004000000010000000042000F010000011842005A0500000004000000010000000042  
005A0500000004000000010000000042007C05000000040000000000000042007901000000404200550500000004000  
0000200000000420091070000002433333364632962392D386537332D346666362D613337622D34323336396635613432

3632000000042007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2B42000D0200000004000000010000000042000F010000006842005C0500000004000000010000000042007F050000000400000000000000042007C010000004042005705000000040000000200000000420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000

1 Client A:  
Get attribute  
In: uuidKey, attributeName={'State'}  
  
Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
  Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
    Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
      Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
      Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
    Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
      Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
      Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
        Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9  
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State  
  
42007501000000A0420074010000003842006701000000204200680200000004000000010000000042006902000000040000000000000042000D0200000004000000010000000042000F010000005842005A050000000400000000B00000000420076010000004042009107000000243333364633962392D386537332D346666362D613337622D343233363966356134323632000000042000A07000000055374617465000000  
  
42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000005842005C050000000400000000B000000004200790100000040420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616461390000000042000A07000000055374617465000000

Out: uuidKey, attribute={ State='00000001' }  
  
Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
  Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
    Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
      Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
      Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
    Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC07820 (Mon Sep 28 0x000000004AFBED2B (Thu Nov 12 12:10:47+28 CEST+35 CET 2009))  
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
    Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
      Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
      Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
      Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
        Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9  
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000001 (Pre-Active)

4200780100000000420077010000000048420067010000002042006802000000040000000100000000420069020000000400000000000042008F090000000800000004AC0782042000D02000000400000001000000042000F010000008042005A050000000400000000000042007C05000000040000000000000000420079010000005842009107000000243333364633962392D386537332D346666362D613337622D34323336396635613432363200000000420008010000002042000A070000000553746174650000042000B0500000004000000010000000042007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000042009209000000800000000400AFBED2B42000D0200000004000000010000000042000F010000008042005C05000000040000000B0000000042007F0500000040000000000000042007C0100000058420094070000002432316432386238612D303664662D343363302D623732662D326131363136333616461390000000420008010000002042000A070000000553746174650000042000B050000040000000100000000

2

Client A:

[Add attribute](#)

[Activate](#)

In: uuidKey, ~~attribute={ ActivationDate='2' }~~

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: ~~0x0000000D (Add Attribute)0x00000012 (Activate)~~

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: ~~333de9b9-8e73-4fff-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9~~

~~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)~~

42007501000000004200740100000038420067010000002042006802000000040000000100000000420069020000000400000000000042008F090000000800000004AC0782042000D02000000400000001000000042000F010000008042005A05000000040000000000000042007C05000000040000000000000000420079010000005842009107000000243333364633962392D386537332D346666362D613337622D34323336396635613432363200000000420008010000002042000A07000000055374617469766174696F6E20446174650042000B0900000008000000000000000002

42007801000000004200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042009209000000800000000400AFBED2B42000D0200000004000000010000000042000F010000008042005C05000000040000000B0000000042007F0500000040000000000000042007C0100000058420094070000002432316432386238612D303664662D343363302D623732662D3261313631363336164613900000000

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

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:

Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: ~~0x00000004AC07820 (Mon Sep~~





Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:

Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: ~~0x000000004AC07820 (Mon-Sep-28-0x000000004AFBED2B (Thu Nov 12 12:10:47+28-CEST35 CET 2009)~~

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)

Tag: Result Status (0x4200760x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: ~~333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9~~

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

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

Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active)

~~42007801000000084200770100000004842006701000000204200680200000004000000010000000042006902000000040000000000000042008F0900000008000000004AC0782042000D02000000400000001000000042000F010000008042005A050000000400000000000000042007C05000000040000000000000004200790100000058420091070000002433333364633962392D386537332D346666362D613337622D34333336396635613432363200000000420098010000002042009A0700000005537461746500000042000B05000000400000002000000042007B01000000D842007A0100000048420069010000002042006A02000000400000001000000042006B020000004000000000000000420092090000008000000004AFBED2B42000D02000000400000001000000042000F010000008042005C0500000040000000B000000042007F05000000400000000000000042007C0100000058420094070000002432316432386238612D303664662D343363302D623732662D3261313631363336164613900000000420008010000002042000A0700000005537461746500000042000B0500000000000000~~

4 Client B:

Locate (symmetric key by name)

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

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

Tag: Request Payload (0x4200760x420079), 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 (0x4200530x420055), Type: Text String (0x07), Data: Key1

Tag: Name Type (0x4200520x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

4200750100000000420074010000003842006701000000204200680200000040000000100000004200690200000040  
0000000000000042000D02000000400000001000000042000F01000008842005A050000004000000080000000042  
00760100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B050000004000  
000020000000420008010000003842000A07000000044E616D65000000042000B010000002042005307000000044B65  
7931000000042005205000000400000010000000

42007801000000004200770100000038420069010000002042006A02000000400000001000000042006B0200000040  
0000000000000042000D02000000400000001000000042000F01000008842005C050000004000000080000000042  
00790100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B050000004000  
000020000000420008010000003842000A07000000044E616D65000000042000B010000002042005507000000044B65  
7931000000042005405000000400000010000000

Out: uuidKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200640x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC07821 (Mon Sep 28 0x000000004AFBED2B (Thu Nov 12 12:10:47:29 CEST35 CET 2009))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Result Status (0x42007C0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9

4200780100000000420077010000004842006701000000204200680200000040000000100000004200690200000040  
0000000000000042008F09000000800000004AC0782142000D02000000400000001000000042000F010000005842  
005A05000000400000008000000042007C050000004000000000000042007901000000304200910700000024333  
33364633962392D386537332D346666362D613337622D343233639663561343236320000000042007B01000000B04200  
7A0100000048420069010000002042006A02000000400000001000000042006B02000000400000000000000042009  
209000000080000000004AFBED2B42000D02000000400000001000000042000F010000005842005C0500000040000000  
080000000042007F05000000400000000000000042007C0100000030420094070000002432316432386238612D30366  
4662D343363302D623732662D32613136313633336164613900000000

5

Client B:  
Get (symmetric key)  
In: uuidKey

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200640x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9

4200750100000000420074010000003842006701000000204200680200000040000000100000004200690200000040  
00000000000042000D02000000400000001000000042000F010000004842005A0500000040000000A000000042  
00760100000030420091070000002433333364633962392D386537332D346666362D613337622D3432333639663561343  
2363200000000

42007801000000904200770100000038420069010000002042006A02000000400000001000000042006B0200000040  
000000000000042000D02000000400000001000000042000F010000004842005C0500000040000000A000000042  
00790100000030420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616  
4613900000000

Out: objectType = '00000002', uuidKey, symmetricKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC07821 (Mon Sep 28 0x000000004AFBED2B (Thu Nov 12 12:10:47+29-EST35 CET 2009))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9  
Tag: Symmetric Key (0x42008E0x42008F), Type: Structure (0x01), Data:  
Tag: Key Block (0x42003E0x420040), Type: Structure (0x01), Data:  
Tag: Key Format Type (0x4200400x420042), Type: Enumeration (0x05), Data: 0x00000001  
Tag: Key Value (0x4200430x420045), Type: Structure (0x01), Data:  
Tag: Key Material (0x4200410x420043), Type: Octet String (0x08), Data: 86C15B28BB6C7A268E9ADEA471A36F23EF7833AB15F5A1EE5874BC0D9BBC4BE7  
Tag: Cryptographic Algorithm (0x4200260x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)  
Tag: Cryptographic Length (0x4200280x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

4200780100000120420077010000004842006701000000204200680200000040000000100000004200690200000040  
00000000000042008F0900000008000000004AC0782142000D02000000400000001000000042000F01000000C842  
005A0500000040000000A000000042007C05000000040000000000000042007901000000A0420055050000004000  
00020000000420091070000002433333364633962392D386537332D346666362D613337622D34323336396635613432  
3632000000042008C010000005842003E0100000050420040050000004000000010000000420043010000001842004  
10800000010E6C15B28BB6C7A268E9ADEA471A36F23420026050000004000000030000000420028020000004000000  
80000000042007B010000012042007A0100000048420069010000002042006A02000000400000001000000042006B0  
2000000040000000000000420092090000008000000004AFBED2B42000D02000000400000001000000042000F01  
000000C842005C0500000040000000A000000042007F050000004000000000000042007C01000000A0420057050  
0000004000000020000000420094070000002432316432386238612D303664662D343363302D623732662D3261313631  
363333616461390000000042008F01000000584200400100000050420042050000004000000010000000042004501000  
000184200430800000010EF7833AB15F5A1EE5874BC0D9BBC4BE7420028050000004000000030000000042002A020000  
00040000008000000000

6 Client B:  
Revoke (symmetric key as compromised)  
In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceTime='6'



In: uuidKey, attributeName={ 'State' }

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9

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

4200750100000000420074010000003842006701000000204200680200000040000000100000000420069020000000400000000000042000D0200000040000000100000004200F010000005842005A0500000040000000B0000000042009107000000243333364633962392D386537332D346666362D613337622D343233363966356134323632000000042000A07000000055374617465000000

42007801000000004200770100000038420069010000002042006A020000004000000010000000042006B020000000400000000000042000D0200000040000000100000004200F010000005842005C0500000040000000B00000000420094070000002432316432386238612D303664662D343363302D623732662D326131363136333361646139000000042000A07000000055374617465000000

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

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:

Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC07822 (Mon Sep 28 0x000000004AFBED2C (Thu Nov 12 12:10:47+30 CEST 2009))

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)

Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9

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

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

Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Compromised)

4200780100000000420077010000004842006701000000204200680200000040000000100000000420069020000000400000000000042008F0900000008000000004AC078224200D02000000400000001000000004200F010000008042009407000000243333364633962392D386537332D346666362D613337622D343233363966356134323632000000042000A0700000005537461746500000042000B050000004000000040000000042007B01000000D842007A0100000048420069010000002042006A02000000400000001000000042006B020000004000000000000042009209000000800000004AFBED2C4200D0200000040000000100000004200F010000008042005C0500000040000000B0000000042007F0

50000000400000000000000042007C0100000058420094070000002432316432386238612D303664662D3433363302D623732662D3261313631363333616461390000000042008010000002042000A0700000005537461746500000042000B050000004000000040000000

8 Client A:

Get attribute list  
In: uuidKey

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9

42007501000000009042007401000000038420067010000002042006802000000040000000100000000420069020000000400000000000042000B02000000040000000010000000042000F010000004842005A05000000040000000000000004200760100000003042009107000000243233364633962392D386537332D346666362D613337622D34323336396635613432363200000000  
420078010000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D02000000040000000010000000042000F010000004842005C050000000400000000000000042007901000000030420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000

Out: uuidKey, attributes = { \* }

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC07822 (Mon Sep 28 0x000000004AFBED2C (Thu Nov 12 12:10:47+30-CEST36 CET 2009))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Compromise Occurrence Date  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Compromise Date

Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digest  
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Initial Date  
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date  
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Revocation Reason  
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Unique Identifier  
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name  
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask  
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type  
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Last [Changed/Change](#) Date

4200780100000228420077010000004842006701000000204200680200000040000000100000004200690200000040  
 000000000000042008F09000000000000004AC0782242000D02000000400000001000000042000F01000001D042  
 005A05000000040000000C0000000042007C0500000004000000000000042007901000001A84200910700000024333  
 33364633962392D386537332D346666362D613337622D3432333639663561343236320000000042000A07000000144372  
 7970746F67726170686963204C655E677468000000042000A070000001743727970746F6772617068696320416C676F7  
 26974686D0042000A0700000005537461746500000042000A070000001A436F6B70726F6D697365204F6363757272656E  
 63652044617465000000000042000A070000000F436F6D70726F6D69736520446174650042000A0700000064469676  
 57374000042000A070000000C496E697469616C2044617465000000042000A07000000F41637469766174696F6E2044  
 6174650042000A07000000115265766F636174696F6E205265617336F6E000000000000042000A0700000011556E69717  
 565204964656E746966696572000000000000042000A07000000044E616D65000000042000A07000000184372797074  
 6F67726170686963205573616765204D61736B42000A070000000B4F626A656374205479706500000000042000A07000  
 000114C617374204368616E676564204461746500000000000042007B010000022042007A0100000048420069010000  
 002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004AFBE  
 D2C42000D020000004000000010000000042000F01000001C842005C05000000040000000C000000042007F05000000  
 040000000000000042007C01000001A04200940700000002432316432386238612D303664662D343363302D623732662  
 D326131363136333616461390000000042000A070000001443727970746F67726170686963204C656E67746800000000  
 42000A070000001743727970746F6772617068696320416C676F726974686D0042000A070000000553746174650000004  
 2000A070000001A436F6D70726F6D697365204F6363757272656E63652044617465000000000042000A070000000F43  
 6F6D70726F6D69736520446174650042000A0700000006446967657374000042000A070000000C496E697469616C20446  
 17465000000042000A070000000F41637469766174696F6E20446174650042000A07000000115265766F636174696F6E  
 20526561736F6E000000000000042000A0700000011556E69717565204964656E746966696572000000000000042000  
 A07000000044E616D65000000042000A070000001843727970746F67726170686963205573616765204D61736B42000A  
 070000000B4F626A656374205479706500000000042000A07000000104C617374204368616E67652044617465

9

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

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
 Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
 Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
 Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
 Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
 Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: [333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9](#)  
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

420075010000000420074010000003842006701000000204200680200000040000000100000004200690200000040  
 000000000000042000D020000004000000010000000042000F010000005842005A05000000040000000B0000000042  
 0076010000004042009107000000243333364633962392D386537332D346666362D613337622D3432333639663561343  
 23632000000042000A07000000055374617465000000



42007801000000A04200770100000038420069010000002042006A020000000400000001000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B000000004200790100000040420094070000002432316432386238612D303664662D343363302D623732662D32613136313633333616461390000000042000A07000000055374617465000000

Out: uuidKey, attribute={ State='0000004' }

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC07822 (Mon Sep 28 0x00000004AFBED2C (Thu Nov 12 12:10:47:30 CEST'36 CET 2009)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9
Tag: Attribute (0x420008), Type: Structure (0x01), Data:
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Compromised)

42007801000000B84200770100000048420067010000002042006802000000040000000100000004200690200000004000000000000042008F0900000008000000004AC0782242000D0200000004000000010000000042000F0100000008042005A05000000040000000B0000000042007C050000000400000000000004200790100000058420091070000002432333364633962392D386537332D346666362D613337622D3432333639663561343236320000000420008010000002042006A0700000005537461746500000042000B050000000400000004000000042007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000000420092090000008000000004AFBED2C42000D0200000004000000010000000042000F010000008042005C05000000040000000B0000000042007F05000000040000000000000042007C0100000058420094070000002432316432386238612D303664662D343363302D623732662D326131363136333336164613900000000420008010000002042000A0700000005537461746500000042000B05000000400000000400000000

10 Client A:
Add attribute [batch]
In: uuidKey, attribute={ x-attribute1='Value1' }
In: uuidKey, attribute={ x-attribute2='Value2' }
Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: 5CD7C98FC5B52FF79D407FFB45C95672
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:





[3D9CF6E0445252B808019A230A05E9E1](#)

Tag: Request Payload ([0x4200760x420079](#)), Type: Structure (0x01), Data:

Tag: Unique Identifier ([0x4200910x420094](#)), Type: Text String (0x07), Data: [333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9](#)

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

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

Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2

[42007501000001704200740100000038420067010000002042006802000000400000001000000042006902000000400000000000042000002000000400000002000000042000F010000009042005A0500000040000000E0000000042009000000008C06597C23E952144420076010000006842009107000000243333364633962392D386537332D346666362D613337622D3432333639663561343236320000000420008010000003042000A070000000C782D61747472696275746531000000042000B070000000E4D6F64696669656456616C756531000042000F010000009042005A0500000040000000E00000000420090000000083D9CF6E0445252B8420076010000006842009107000000243333364633962392D386537332D346666362D613337622D3432333639663561343236320000000420008010000003042000A070000000C782D61747472696275746532000000042000B070000000E4D6F64696669656456616C7565320000](#)

[42007801000001704200770100000038420069010000002042006A02000000400000001000000042006B020000004000000000000420000020000000400000002000000042000F010000009042005C0500000040000000E00000000420093080000000847FB42CCECA3F6EC4200790100000068420094070000002432316432386238612D303664662D343363302D623732662D326131363136333616461390000000420008010000003042000A070000000C782D61747472696275746531000000042000B070000000E4D6F64696669656456616C756531000042000F010000009042005C0500000040000000E00000000420093080000000808019A230A05E9E14200790100000068420094070000002432316432386238612D303664662D343363302D623732662D326131363136333616461390000000420008010000003042000A070000000C782D61747472696275746532000000042000B070000000E4D6F64696669656456616C7565320000](#)

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

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

Tag: Response Message ([0x4200780x42007B](#)), Type: Structure (0x01), Data:

Tag: Response Header ([0x4200770x42007A](#)), Type: Structure (0x01), Data:

Tag: Protocol Version ([0x4200670x420069](#)), Type: Structure (0x01), Data:

Tag: Protocol Version Major ([0x4200680x42006A](#)), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor ([0x4200690x42006B](#)), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp ([0x42008F0x420092](#)), Type: Date-Time (0x09), Data: [0x00000004AC07823 \(Mon Sep 28 0x000000004AFBED2D \(Thu Nov 12 12:10:47+31-CEST37 CET 2009\)](#)

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

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

Tag: Operation ([0x42005A0x42005C](#)), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)

Tag: Unique Batch Item ID ([0x4200900x420093](#)), Type: Octet String (0x08), Data: [C06597C23C95214447FB42CCECA3F6EC](#)

Tag: Result Status ([0x42007C0x42007F](#)), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload ([0x4200790x42007C](#)), Type: Structure (0x01), Data:

Tag: Unique Identifier ([0x4200910x420094](#)), Type: Text String (0x07), Data: [333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9](#)

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

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

Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1

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

Tag: Operation ([0x42005A0x42005C](#)), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)

Tag: Unique Batch Item ID ([0x4200900x420093](#)), Type: Octet String (0x08), Data: [3D9CF6E0445252B808019A230A05E9E1](#)

Tag: Result Status ([0x42007C0x42007F](#)), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload ([0x4200790x42007C](#)), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9

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

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

Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2

42007801000001A04200770100000048420067010000002042006802000000400000001000000042006902000000400000000000042008F090000000800000004AC0782342000D02000000400000002000000042000F01000000A042005A05000000400000004200900800000008C06597C23C95214442007C05000000400000000000004200790100000068420091070000002433333364633962392D386537332D346666362D613337622D343233363966356134323632000000042008010000003042000A070000000C782D61747472696275746531000000042000B07000000E4D6F64696669656456616C756532000042000F01000000A042005A0500000040000000E00000004200900800000083D9CF6E0445252B842007C0500000040000000000000420079010000006842009107000000243333364633962392D386537332D346666362D613337622D343233363966356134323632000000042008010000003042000A070000000C782D6174747269627574653200000042000B07000000E4D6F64696669656456616C756532000042007B01000001A042007A010000048420069010000002042006A0200000004000000010000000042006B0200000040000000000000004200920900000800000004AFBED2D42000D020000000400000002000000042000F01000000A042005C0500000040000000E000000042009308000000847FB42CCECA3F6EC42007F0500000040000000000000042007C0100000068420094070000002432316432386238612D303664662D343363302D623732662D326131363136333616461390000000420008010000003042000A070000000C782D61747472696275746531000000042000B07000000E4D6F64696669656456616C75653100042000F01000000A042005C0500000040000000E000000042009308000000808019A230A05E9E142007F0500000004000000000000042007C0100000068420094070000002432316432386238612D303664662D343363302D623732662D326131363136333616461390000000420008010000003042000A070000000C782D61747472696275746532000000042000B07000000E4D6F64696669656456616C7565320000

12

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

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)

Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: 1A1B48172DF57ABC3E2C080FA8806057

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)

Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data: B77FB0753B7C95EB9D5598D43D23B82

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9

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

42007501000001304200740100000038420067010000002042006802000000400000001000000042006902000000400000000000042008F090000000800000004AC0782342000D02000000400000002000000042000F01000000A042005A0500000040000000E00000004200900800000008C06597C23C95214442007C05000000400000000000004200790100000068420091070000002433333364633962392D386537332D346666362D613337622D343233363966356134323632000000042008010000003042000A070000000C782D61747472696275746531000000042000B07000000E4D6F64696669656456616C756532000042007B01000001A042007A010000048420069010000002042006A0200000004000000010000000042006B0200000040000000000000004200920900000800000004AFBED2D42000D020000000400000002000000042000F01000000A042005C0500000040000000E000000042009308000000847FB42CCECA3F6EC42007F0500000040000000000000042007C0100000068420094070000002432316432386238612D303664662D343363302D623732662D326131363136333616461390000000420008010000003042000A070000000C782D61747472696275746532000000042000B07000000E4D6F64696669656456616C7565320000

00000000000081A1B48172DF57ABC420076010000004842009107000000243333364633962392D386537332D346666  
62D613337622D3432333639663561343236320000000042000A070000000C782D61747472696275746531000000004200  
0F010000007042005A0500000004000000F000000004200900800000008B77FD0753B7C95ED420076010000004842009  
107000000243333364633962392D386537332D346666362D613337622D343233363966356134323632000000004200A  
070000000C782D6174747269627574653200000000

42007801000001304200770100000038420069010000002042006A020000000400000001000000042006B02000000040  
0000000000000042000D0200000004000000020000000042000F010000007042005C05000000040000000F0000000042  
009308000000083E2C080FA88060574200790100000048420094070000002432316432386238612D303664662D3433633  
02D623732662D3261313631363333616461390000000042000A070000000C782D61747472696275746531000000004200  
0F010000007042005C05000000040000000F000000004200930800000089D55988D43D23B82420079010000004842009  
4070000002432316432386238612D303664662D343363302D623732662D326131363136333361646139000000004200A  
070000000C782D6174747269627574653200000000

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

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

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:

Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200690x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: ~~0x000000004AC07826 (Mon Sep 28 0x0000000004AFBED2D (Thu Nov 12 12:10:47+34 CEST 2009))~~

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)

Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data:

~~1A1B48172DF57ABC3E2C080FA8806057~~

Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: ~~333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9~~

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

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

Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)

Tag: Unique Batch Item ID (0x4200900x420093), Type: Octet String (0x08), Data:

~~B77FD0753B7C95ED9D55988D43D23B82~~

Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: ~~333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9~~

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

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

Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2

42007801000001A042007701000000484200690100000020420068020000000400000001000000042006902000000040  
00000000000000420008F0900000008000000004AC0782642000D0200000004000000020000000042000F01000000A042  
005A05000000040000000F00000000420090080000000081A1B48172DF57ABC42007C0500000004000000000000420  
079010000006842009107000000243333364633962392D386537332D346666362D613337622D34323336396635613432  
363200000000420008010000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F6

4696669656456616C756531000042000F01000000A042005A0500000004000000F00000000420090800000008B77FD0  
753B7C95ED42007C050000000400000000000000420079010000006842009107000000243333364633962392D38653  
7332D346666362D613337622D3433333639663561343236320000000420008010000003042000A070000000C782D6174  
7472696275746532000000042000B070000000E4D6F64696669656456616C756532000042007B01000001A042007A010  
0000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000004200920900  
00000800000004AFBED2D42000D020000000400000002000000042000F01000000A042005C05000000040000000F000  
000004200930800000083E2C080FA880605742007F050000000400000000000000042007C0100000068420094070000  
002432316432386238612D303664662D343363302D623732662D326131363136333361646139000000004200080100000  
03042000A070000000C782D617474726962757465310000000042000B070000000E4D6F64696669656456616C75653100  
0042000F01000000A042005C05000000040000000F000000004200930800000089D55988D43D23B8242007F050000000  
40000000000000042007C0100000068420094070000002432316432386238612D303664662D343363302D623732662D  
3261313631363336164613900000000420008010000003042000A070000000C782D6174747269627574653200000004  
2000B070000000E4D6F64696669656456616C7565320000

13

Client A:

Get (symmetric key)

In: uuidKey

Tag: Request Message ([0x4200750x420078](#)), Type: Structure (0x01), Data:

Tag: Request Header ([0x4200740x420077](#)), Type: Structure (0x01), Data:

Tag: Protocol Version ([0x4200670x420069](#)), Type: Structure (0x01), Data:

Tag: Protocol Version Major ([0x4200680x42006A](#)), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor ([0x4200690x42006B](#)), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation ([0x42005A0x42005C](#)), Type: Enumeration (0x05), Data: 0x0000000A (Get)

Tag: Request Payload ([0x4200760x420079](#)), Type: Structure (0x01), Data:

Tag: Unique Identifier ([0x4200910x420094](#)), Type: Text String (0x07), Data: [333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9](#)

[4200750100000090420074010000003842006701000000204200680200000004000000010000000042006902000000040  
0000000000000042000D0200000004000000010000000042000F01000000A042005A05000000040000000A0000000042  
0076010000003042009107000000243333364633962392D386537332D346666362D613337622D3433333639663561343  
23632000000000](#)

[42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040  
0000000000000042000D0200000004000000010000000042000F01000000A042005C05000000040000000A0000000042  
00790100000030420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616  
46139000000000](#)

Out: objectType = '00000002', uuidKey, symmetricKey

Tag: Response Message ([0x4200780x42007B](#)), Type: Structure (0x01), Data:

Tag: Response Header ([0x4200770x42007A](#)), Type: Structure (0x01), Data:

Tag: Protocol Version ([0x4200670x420069](#)), Type: Structure (0x01), Data:

Tag: Protocol Version Major ([0x4200680x42006A](#)), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor ([0x4200690x42006B](#)), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp ([0x42008F0x420092](#)), Type: Date-Time (0x09), Data: [0x000000004AC07827 \(Mon Sep 28 0x000000004AFBED2D \(Thu Nov 12 12:10:47:35 CEST 2009\)\)](#)

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

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

Tag: Operation ([0x42005A0x42005C](#)), Type: Enumeration (0x05), Data: 0x0000000A (Get)

Tag: Result Status ([0x4200760x42007F](#)), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload ([0x4200790x42007C](#)), Type: Structure (0x01), Data:

Tag: Object Type ([0x4200550x420057](#)), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

	<p>Tag: Unique Identifier (<a href="#">0x4200910x420094</a>), Type: Text String (0x07), Data: <a href="#">333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9</a></p> <p>Tag: Symmetric Key (<a href="#">0x420080x42008F</a>), Type: Structure (0x01), Data:</p> <p>Tag: Key Block (<a href="#">0x42003F0x420040</a>), Type: Structure (0x01), Data:</p> <p>Tag: Key Format Type (<a href="#">0x420040x420042</a>), Type: Enumeration (0x05), Data: 0x00000001</p> <p>Tag: Key Value (<a href="#">0x4200430x420045</a>), Type: Structure (0x01), Data:</p> <p>Tag: Key Material (<a href="#">0x4200410x420043</a>), Type: Octet String (0x08), Data: <a href="#">E6C15B28BB6C7A268E9ADEA471A36F23EF7833AB15F5A1EE5874BC0D9BBC4BE7</a></p> <p>Tag: Cryptographic Algorithm (<a href="#">0x4200260x420028</a>), Type: Enumeration (0x05), Data: 0x00000003 (AES)</p> <p>Tag: Cryptographic Length (<a href="#">0x4200280x42002A</a>), Type: Integer (0x02), Data: 0x00000080 (128)</p> <p><a href="#">4200780100000012042007701000000484200670100000020420068020000004000000010000000420069020000000400000000000042008F090000000800000004AC0782742000D02000000400000001000000042000F01000000C842005A0500000040000000A000000042007C05000000040000000000000042007901000000A042005505000000400000000000042009107000000243333364633962392D386537332D346666362D613337622D343233363966356134323632000000042008E010000005842003E010000005042004005000000400000001000000042004301000000184200410800000010E6C15B28BB6C7A268E9ADEA471A36F234200260500000040000000300000004200280200000040000008000000042007B010000012042007A0100000048420069010000002042006A02000000400000001000000042006B0200000040000000000000420092090000008000000004AFBED2D42000D02000000400000001000000042000F01000000C842005C0500000040000000A000000042007F05000000400000000000000042007C01000000A0420057050000004000000020000000420094070000002432316432386238612D303664662D343363302D623732662D32613136313633361646139000000042008F010000005842004001000000504200420500000040000000100000004200450100000184200430800000010EF7833AB15F5A1EE5874BC0D9BBC4BE742002805000000400000003000000042002A02000000400000008000000000</a></p>
14	<p>Client A:</p> <p>Destroy (symmetric key)</p> <p>In: uuidKey</p> <p>Tag: Request Message (<a href="#">0x4200750x420078</a>), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (<a href="#">0x4200740x420077</a>), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (<a href="#">0x4200670x420069</a>), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (<a href="#">0x4200680x42006A</a>), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (<a href="#">0x4200690x42006B</a>), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (<a href="#">0x42005A0x42005C</a>), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</p> <p>Tag: Request Payload (<a href="#">0x4200760x420079</a>), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (<a href="#">0x4200910x420094</a>), Type: Text String (0x07), Data: <a href="#">333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9</a></p> <p><a href="#">420075010000009042007401000000384200670100000020420068020000004000000010000000420069020000000400000000000042000D02000000400000004000000042000F010000004842005A050000004000000140000000420076010000003042009107000000243333364633962392D386537332D346666362D613337622D34323336396635613432363200000000</a></p> <p><a href="#">42007801000000904200770100000038420069010000002042006A02000000400000001000000042006B020000000400000000000042000D02000000400000004000000042000F010000004842005C0500000040000001400000004200790100000030420094070000002432316432386238612D303664662D343363302D623732662D3261313631363336164613900000000</a></p> <p>Out: uuidKey</p> <p>Tag: Response Message (<a href="#">0x4200780x42007B</a>), Type: Structure (0x01), Data:</p> <p>Tag: Response Header (<a href="#">0x4200770x42007A</a>), Type: Structure (0x01), Data:</p>



Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
 Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC07827 (Mon Sep 28 0x000000004AFBED2E (Thu Nov 12 12:10:47:35 CEST38 CET 2009))  
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
 Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
 Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
 Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
 Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 333de9b9-8e73-4ff6-a37b-42369f5a426221d28b8a-06df-43c0-b72f-2a161633ada9

42007801000000B04200770100000048420067010000002042006802000000040000000100000000420069020000000400000000000042008F0900000008000000004AC0782742009D020000004000000010000000042009F010000005842005A0500000004000000140000000042007C050000000400000000000000004200790100000030420091070000002433323364633962392D386537332D346666362D613337622D3432333639663561343236320000000042007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000000004200920900000008000000004AFBED2E42000D0200000004000000010000000042009F010000005842005C0500000004000000140000000042007F05000000040000000000000042007C0100000030420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000

125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137

## 55 Auditing and reporting

### 5.15.1 Use-case: Get usage allocation scenario

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

Formatted: Style Heading 1h1Level 1 Topic Heading + Before: 5 pt After: 5..., Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 3 + Alignment: Left + Aligned at: 0 pt + Indent at: 0 pt

Formatted: Indent: Left: 0 pt, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 36 pt + Indent at: 36 pt, Don't adjust space between Latin and Asian text

Formatted: Font: Not Bold

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 (0x4200750x420078), Type: Structure (0x01), Data: Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Template-Attribute (0x42008E0x420091), 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 (0x4200530x420055), Type: Text String (0x07), Data: Key1  
Tag: Name Type (0x4200520x420054), 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)

-----  
420075010000016042007401000000384200670100000020420068020000004000000010000000042006902000000400  
00000000000042000D0200000004000000010000000042000F010000011842005A0500000040000000100000004200  
7601000001004200550500000004000000020000000042008E01000000E8420008010000003042000A0700000017437279  
70746F6772617068696320416C676F726974686D0042000B050000004000000030000000420008010000003042000A07  
000001443727970746F67726170686963204C656E677468000000042000B02000000400000008000000004200080100  
00003842000A07000000044E616D65000000042000B01000000204200530700000044B6579310000000420052050000  
00040000000100000000420008010000003042000A070000001843727970746F67726170686963205573616765204D6173  
6B42000B02000000040000000400000000

42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B02000000400  
000000000000042000D0200000004000000010000000042000F010000011842005C0500000040000000100000004200  
7901000001004200570500000004000000020000000042009101000000E8420008010000003042000A0700000017437279  
70746F6772617068696320416C676F726974686D0042000B050000004000000030000000420008010000003042000A07  
000001443727970746F67726170686963204C656E677468000000042000B02000000400000008000000004200080100  
00003842000A07000000044E616D65000000042000B01000000204200550700000044B6579310000000420054050000  
00040000000100000000420008010000003042000A070000001843727970746F67726170686963205573616765204D6173  
6B42000B02000000040000000400000000

Formatted: Font color: Black

Out: objectType = '00000002', uuidKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC07828 (Mon Sep 28 10:47:36 CEST 2009)0x000000004B98E05A (Thu Mar 11 13:21:46 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: ~~4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29ba1d~~

-----

42007801000000004200770100000048420067010000002042006802000000400000001000000042006902000000400000000000042008F0900000000800000004AC0782842000D02000000400000001000000042000F010000006842005A05000000400000001000000042007C05000000040000000000000042007901000000404200550500000040000000020000000420091070000002434666563336135392D623231372D346162662D383461642D616663135343730323436313500000042007B01000000C042007A0100000048420069010000002042006A020000004000000010000000042006B02000000400000000000000042009209000000800000004B98E05A42000D02000000400000001000000042000F010000006842005C05000000400000001000000042007F050000004000000000000042007C01000000404200570500000004000000020000000420094070000002465363936656264302D386562612D343036652D626532312D64393035396532396261316400000000

Formatted: Font color: Black

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

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)  
Tag: Unique Batch Item ID (0x4200990x420093), Type: Octet String (0x08), Data: ~~E1AE8A5206CC749AD7FE2477E364AE1A~~  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: ~~4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29ba1d~~  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date  
Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000000000002 (Thu Jan 01 01:00:02 CET 1970)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)  
Tag: Unique Batch Item ID (0x4200990x420093), Type: Octet String (0x08), Data: ~~C6CAA6E0C409336F9696012991BC8A59~~  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: ~~4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29ba1d~~  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date  
Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: ~~0x00000004AC07A80 (Mon Sep 28 10:57:36 CEST 20090x00000004B98E2B3 (Thu Mar 11 13:31:47 CET 2010)~~

-----

420075010000001684200740100000038420067010000002042006802000000400000001000000042006902000000400000000000042008F0900000000800000004AC0782842000D02000000400000001000000042000F010000006842005A05000000400000001000000042007C05000000040000000000000042007901000000404200550500000040000000020000000420091070000002434666563336135392D623231372D346162662D383461642D6166631353437303234363135000000004200801000000002842000A070000000F41637469766174696F6E204461746500420008090000000000000000000000242000F010000009042005A0500000040000000D00000000420090080000008C6AA6E0C409336F4200760100000068420091070000002434666563336135392D623231372D346162662D383461642D61666313534373032343631350000000042008010000003042000A070000001150726F746563742053746F70204461746500000000000042000B09000000800000004AC07A80

42007801000001684200770100000038420069010000002042006A02000000400000001000000042006B02000000400

Formatted: Font color: Black

00000000000042000D0200000040000002000000042000F01000008842005C050000004000000D00000004200  
930800000008D7FE2477E364AE1A420079010000006042009407000002465363936656264302D386562612D343036652D  
626532312D6439303539653239626131640000000420008010000002842000A07000000F41637469766174696F6E2044  
6174650042000B09000000800000000000000242000F01000009042005C050000004000000D00000004200930800  
0000089696012991BC8A59420079010000006842009407000002465363936656264302D386562612D343036652D626532  
312D6439303539653239626131640000000420008010000003042000A070000001150726F746563742053746F70204461  
74650000000000042000B090000008000000004B98E2B3

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

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC07828 (Mon-Sep-28-10-00:00:00:0004B98E05B (Thu Mar 11 13:21:47+36-CEST-2009 CET 2010))  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)  
Tag: Unique Batch Item ID (0x4200940x420093), Type: Octet String (0x08), Data: E1AE8A5206CC749AD7FE2477E364AE1A  
Tag: Result Status (0x42007C0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29ba1d  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date  
Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000000000002 (Thu Jan 01 01:00:02 CET 1970)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)  
Tag: Unique Batch Item ID (0x4200940x420093), Type: Octet String (0x08), Data: C6CAA6E0C409336F9696012991BC8A59  
Tag: Result Status (0x42007C0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29ba1d  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date  
Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004AC07A80 (Mon-Sep-28-10-57:36-CEST-2009)0x000000004B98E2B3 (Thu Mar 11 13:31:47 CET 2010)

-----  
420078010000019842007701000000484200670100000020420068020000004000000010000000420069020000000400  
00000000000042008F09000000008000000004AC0782842000D020000000400000020000000042000F01000000984200  
5A050000004090000000000000000000004200908000000008E1AE8A5206CC749A42007C050000000400000000000000420079  
0100000060420091070000002434666563336135392D623231372D346162662B383461642D616631353437303234363135  
0000000420008010000002842000A07000000F41637469766174696F6E20446174650042000B090000008000000000  
00000242000F01000000A042005A0500000040000000D00000004200908000000008C6CAA6E0C409336F42007C050000  
00040000000000000004200790100000068420091070000002434666563336135392D623231372D346162662B38346164  
2D61663135343730323436313500000000420008010000003042000A070000001150726F746563742053746F7020446174  
650000000000042000B090000008000000004AC07A8042007B010000019842007A0100000048420069010000002042  
006A020000004000000010000000042006B020000004000000000000000420092090000008000000004B98E05B4200  
0D020000004000000020000000042000F010000009842005C050000004000000D00000004200930800000008D7FE24  
77E364AE1A42007F0500000040000000000000042007C0100000060420094070000002465363936656264302D386562

Formatted: Font color: Black



```

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:
  Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-
  4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29bald
  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
    Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Usage Limits
    Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
      Tag: Usage Limits Total Bytes (0x420095(0x420097), Type: BigLong Integer (0x040x03),
      Data: 0000000000003E80x000000000000003E8 (1000)
      Tag: Usage Limits Byte-Count (0x4200930x420096), Type: BigLong Integer (0x040x03), Data:
      0000000000003E80x000000000000003E8 (1000)

42007801000000F842007701000000484200670100000020420068020000004000000010000000042006902000000400
00000000000042008F090000000800000004AC6782A42000D02000000400000010000000042009F01000000A04200
5A0500000004000000B0000000042007C050000000400000000000000042007901000000784200910700000024346665
63336135392D623231372D346162662D383461642D6166313534373032343631350000000042008010000004042000A07
0000000C5573616765204C696D697473000000004200B0100000020420095040000008000000000003E84200930400
00000000000000003E8 Tag: Usage Limits Unit (0x420098), Type: Enumeration (0x05), Data:
0x00000001 (Byte)

42007B010000010842007A0100000048420069010000002042006A020000000400000001000000042006B02000000400
00000000000004200920900000008000000004B98E05C42000D020000004000000010000000042000F01000000B04200
5C0500000004000000D0000000042007F0500000004000000000000000000042007C01000000884200940700000024653639
36656264302D386562612D343036652D626532312D6439303539653239626131640000000042008010000005042000A07
0000000C5573616765204C696D697473000000004200B010000003042009703000000800000000000003E84200960300
0000080000000000003E842009805000000040000000100000000

```

```

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

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
    Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
      Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
      Tag: Request Payload (0x4200760x420079), 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 (0x4200530x420055), Type: Text String (0x07), Data: Key1
            Tag: Name Type (0x4200520x420054), Type: Enumeration (0x05), Data: 0x00000001
            (Uninterpreted text string)

-----
42007501000000D042007401000000384200670100000020420068020000004000000010000000042006902000000400
00000000000042008F0200000004000000010000000042009F010000008842005A05000000040000008000000004200
76010000007042008010000002842000A070000000B4F626A65637420547970650000000004200B0500000004000000

```

Formatted: Font color: Black

020000000420008010000003842000A07000000044E616D65000000042000B010000002042005307000000044B6579310000000042005205000000040000000100000000

42007801000000D04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000042000D020000000400000001000000042000F010000008842005C05000000040000000800000004200790100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000020000000420008010000003842000A07000000044E616D65000000042000B010000002042005307000000044B657931000000042005405000000040000000100000000

Out: uuidKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0782A (Mon-Sep-28-10-47-38-CEST-2009)x000000004B98E05C (Thu Mar 11 13:21:48 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29bald

Formatted: Font color: Black

42007801000000B042007701000000484200670100000020420068020000000400000001000000004200690200000004000000000000042008F090000000800000004AC0782A42000D0200000004000000010000000042000F010000005842005A050000000400000008000000042007C05000000040000000000000004200790100000030420091070000002434666563336135392D623231372D346162662D383461642D616631353437303234363135000000042007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000800000004B98E05C42000D0200000004000000010000000042000F010000005842005C05000000040000000800000042007F05000000040000000000000042007C0100000030420094070000002465363936656264302D386562612D343036652D626532312D64393035396532396261316400000000

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

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29bald

Formatted: Font color: Black

4200750100000090420074010000003842006701000000204200680200000004000000010000000042006902000000040000000000042008F090000000800000004AC0782A42000D0200000004000000010000000042000F010000005842005A050000000400000008000000042007C05000000040000000000000004200790100000030420091070000002434666563336135392D623231372D346162662D383461642D61663135343730323436313500000000

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B020000000400  
0000000000004200D0200000004000000010000000042000F010000004842005C05000000040000000A000000004200  
790100000030420094070000002465363936656264302D386562612D343036652D626532312D6439303539653239626131  
6400000000

Out: objectType = '00000002', uuidKey, symmetricKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0782A (Mon Sep 28 10:47:38 CEST 2009)x000000004B98E05C (Thu Mar 11 13:21:48 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Result Status (0x42007C0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29ba1d  
Tag: Symmetric Key (0x42008E0x42008F), Type: Structure (0x01), Data:  
Tag: Key Block (0x42003E0x420040), Type: Structure (0x01), Data:  
Tag: Key Format Type (0x4200400x420042), Type: Enumeration (0x05), Data: 0x00000001  
Tag: Key Value (0x4200430x420045), Type: Structure (0x01), Data:  
Tag: Key Material (0x4200410x420043), Type: Octet String (0x08), Data: 3D41DF1C5C20E272212D86D762A8C7D4674B32B1A3266DF1253B0F2C4440B0B0  
Tag: Cryptographic Algorithm (0x4200260x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)  
Tag: Cryptographic Length (0x4200280x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

-----  
42007801000001204200770100000048420067010000002042006802000000040000000100000000420069020000000400  
00000000000042008F090000000800000004AC0782A42000D0200000004000000010000000042000F010000000C84200  
5A05000000040000000A00000000042007C05000000004000000000000000420079010000000A04200550500000004000000  
020000000042009107000000243466656336135392D623231372D346162662D383461642D616631353437303234363135  
0000000042008C010000005842003E01000000504200400500000004000000010000000042004301000000184200410800  
0000103D41DF1C5C20E272212D86D762A8C7D4420026050000004000000030000000420028020000004000000800000  
000042007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000  
04000000000000004200920900000008000000004B98E05C42000D0200000004000000010000000042000F010000000C8  
42005C05000000040000000A0000000042007F0500000004000000000000000042007C010000000A0420057050000000400  
0000200000000420094070000002465363936656264302D386562612D343036652D626532312D64393035396532396261  
31640000000042008F01000000584200400100000050420042050000000400000001000000004200450100000018420043  
0800000010674B32B1A3266DF1253B0F2C4440B0B04200280500000004000000030000000042002A020000000400000080  
00000000

Formatted: Font color: Black

5	Client B: <a href="#">Check</a> Get usage allocation In (header): <a href="#">BatchOrderOption='true'</a> In: uuidKey, <a href="#">UsageLimitsByteCount=UsageLimitsCount='500'</a> In: <a href="#">uuidKey, UsageLimitsCount='500'</a>
---	---



Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) (0x00000002 (2))  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) (0x00000009 (Check))  
Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 19D4F3DC9635307A  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29ba1d  
Tag: Usage Limits Byte-Count (0x4200930x420096), Type: BigLong Integer (0x04), Data: 01F4 (500)

42007501000000A04200740100000038420067010000002042006802000000040000000100000000420069020000000400000000000042006B02000000040000000042006A010000005842005A050000000400000011000000004200760100000040420091070000002434666563336135392D623231372D346162662D383461642D6166313534373032343631350000000042009304000000080000000000000001F4

Out: uuidKey

Tag: Response Message (0x420078), Type: Structure (0x010x03), Data: 0x00000000000001F4 (500)  
Tag: Response Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420067), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F), Type: Date-Time (0x09), Data: 0x00000004AC0782A (Mon Sep 28 10:47:38 CEST 2009)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)  
Tag: Result-Status (0x42007C) Unique Batch Item ID (0x420093), Type: Enumeration (0x05) Octet String (0x08), Data: 0x00000000 (Success) 20C8DFFD55BDEE8  
Tag: ResponseRequest Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29ba1d

42007801000000B04200770100000048420067010000002042006802000000040000000100000000420069020000000400000000000042006A010000005842005A050000000400000011000000004200760100000040420091070000002434666563336135392D623231372D346162662D383461642D61663135343730323436313500000000 Tag: Usage Limits Count (0x420096), Type: Long Integer (0x03), Data: 0x00000000000001F4 (500)

420078010000001204200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042006B02000000040000000042000F010000006842005C05000000040000000900000000420093080000000819D4F3DC9635307A4200790100000040420094070000002465363936656264302D386562612D343036652D626532312D64393035396532396261316400000004200960300000080000000000001F44200F010000006842005C050000004000000110000000420093080000000820C8DFFD55BDEE84200790100000040420094070000002465363936656264302D386562612D343036652D626532312D6439303539653239626131640000000420096030000008000000000000001F4

[Out: uuidKey](#)

[Out: uuidKey](#)

[Tag: Response Message \(0x42007B\), Type: Structure \(0x01\), Data:](#)

[Tag: Response Header \(0x42007A\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version \(0x420069\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version Major \(0x42006A\), Type: Integer \(0x02\), Data: 0x00000001 \(1\)](#)

[Tag: Protocol Version Minor \(0x42006B\), Type: Integer \(0x02\), Data: 0x00000000 \(0\)](#)

[Tag: Time Stamp \(0x420092\), Type: Date-Time \(0x09\), Data: 0x00000004B98E05D \(Thu Mar 11 13:21:49 CET 2010\)](#)

[Tag: Batch Count \(0x42000D\), Type: Integer \(0x02\), Data: 0x00000002 \(2\)](#)

[Tag: Batch Item \(0x42000F\), Type: Structure \(0x01\), Data:](#)

[Tag: Operation \(0x42005C\), Type: Enumeration \(0x05\), Data: 0x00000009 \(Check\)](#)

[Tag: Unique Batch Item ID \(0x420093\), Type: Octet String \(0x08\), Data: 19D4F3DC9635307A](#)

[Tag: Result Status \(0x42007F\), Type: Enumeration \(0x05\), Data: 0x00000000 \(Success\)](#)

[Tag: Response Payload \(0x42007C\), Type: Structure \(0x01\), Data:](#)

[Tag: Unique Identifier \(0x420094\), Type: Text String \(0x07\), Data: e696ebd0-8eba-406e-be21-d9059e29bald](#)

[Tag: Batch Item \(0x42000F\), Type: Structure \(0x01\), Data:](#)

[Tag: Operation \(0x42005C\), Type: Enumeration \(0x05\), Data: 0x00000011 \(Get Usage Allocation\)](#)

[Tag: Unique Batch Item ID \(0x420093\), Type: Octet String \(0x08\), Data: 20C8DFFD55BDEEE8](#)

[Tag: Result Status \(0x42007F\), Type: Enumeration \(0x05\), Data: 0x00000000 \(Success\)](#)

[Tag: Response Payload \(0x42007C\), Type: Structure \(0x01\), Data:](#)

[Tag: Unique Identifier \(0x420094\), Type: Text String \(0x07\), Data: e696ebd0-8eba-406e-be21-d9059e29bald](#)

42007B010000013042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B98E05D42000D02000000040000000020000000042000F010000006842005C05000000040000000900000000420093080000000819D4F3DC9635307A42007F05000000040000000000000042007C0100000030420094070000002465363936656264302D386562612D343036652D626532312D6439303539653239626131640000000042000F010000006842005C05000000040000001100000000420093080000000820C8DFFD55BDEEE842007F05000000400000000000000042007C0100000030420094070000002465363936656264302D386562612D343036652D626532312D64393035396532396261316400000000

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

6

Client A:

Get usage allocation

In: uuidKey, [UsageLimitsByteCountUsageLimitsCount](#)='500'

[Tag: Request Message \(0x4200750x420078\), Type: Structure \(0x01\), Data:](#)

[Tag: Request Header \(0x4200740x420077\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version \(0x4200670x420069\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version Major \(0x4200680x42006A\), Type: Integer \(0x02\), Data: 0x00000001 \(1\)](#)

[Tag: Protocol Version Minor \(0x4200690x42006B\), Type: Integer \(0x02\), Data: 0x00000000 \(0\)](#)

[Tag: Batch Count \(0x42000D\), Type: Integer \(0x02\), Data: 0x00000001 \(1\)](#)

[Tag: Batch Item \(0x42000F\), Type: Structure \(0x01\), Data:](#)

[Tag: Operation \(0x42005A0x42005C\), Type: Enumeration \(0x05\), Data: 0x00000011 \(Get Usage Allocation\)](#)

[Tag: Request Payload \(0x4200760x420079\), Type: Structure \(0x01\), Data:](#)

[Tag: Unique Identifier \(0x4200910x420094\), Type: Text String \(0x07\), Data: 4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29bald](#)

[Tag: Usage Limits \[Byte\]\(#\) Count \(0x4200930x420096\), Type: \[BigLong\]\(#\) Integer \(0x040x03\), Data:](#)

01F40x0000000000001F4 (500)

42007501000000A04200770100000038420067010000002042006802000000400000001000000004200690200000040000000000042000D0200000004000000010000000042000F010000005842005A050000000400000011000000004200760100000040420091070000002434666563336135392D623231372D346162662D383461642D616663135343730323436313500000000420093040000000800000000000000001F4

Formatted: Font color: Black

Out: uuidKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0782B (Mon Sep 28 10:47:39 CEST 2009)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)
Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29ba1d

Formatted: Font color: Black

42007801000000B04200770100000048420067010000002042006802000000400000001000000004200690200000040000000000042000D020000000042000F09000000008000000004AC0782B42000D02000000040000000042000F010000005842005A050000000400000001000000004200790100000030420091070000002434666563336135392D623231372D346162662D383461642D61666313534373032343631350000000042007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000000420092090000008000000004B98E05D42000D0200000004000000010000000042000F010000005842005C0500000004000000110000000042007F05000000040000000000000042007C0100000030420094070000002465363936656264302D386562612D343036652D626532312D64393035396532396261316400000000

7 Client C:
Locate (symmetric key by name)
In: objectType = '0000002', attributes={ Name={ Name='Key1', NameType='0000001'}}
Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
Tag: Request Payload (0x4200760x420079), 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 (0x4200530x420055), Type: Text String (0x07), Data: Key1  
 Tag: Name Type (0x4200520x420054), Type: Enumeration (0x05), Data: 0x00000001  
 (Uninterpreted text string)

-----  
 42007501000000D042007401000000384200670100000020420068020000004000000010000000042006902000000400  
 000000000000042000B0200000004000000010000000042000F010000008842005A050000000400000008000000004200  
 760100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000  
 0200000000420008010000003842000A07000000044E616D65000000042000B010000002042005307000000044B657931  
 0000000042005205000000040000000100000000  
 42007801000000D04200770100000038420069010000002042006A0200000004000000010000000042006B020000000400  
 000000000000042000D0200000004000000010000000042000F010000008842005C050000000400000008000000004200  
 790100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000  
 0200000000420008010000003842000A07000000044E616D65000000042000B010000002042005507000000044B657931  
 0000000042005405000000040000000100000000

Formatted: Font color: Black

Out: uuidKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
 Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
 Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
 Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0782B (Mon-Sep  
 28 10:47:39 CEST 2009)0x000000004B98E05D (Thu Mar 11 13:21:49 CET 2010)  
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
 Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
 Tag: Result Status (0x42007C0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
 Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
 Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-  
 4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29ba1d

-----  
 42007801000000D04200770100000048420067010000002042006802000000040000000100000000420069020000000400  
 000000000000042000F0900000000800000004AC0782B42000B0200000004000000010000000042000F01000000584200  
 5A0500000004000000080000000042007C05000000040000000000000042007901000000304200910700000024346665  
 63336135392D623231372D346162662D383461642D6166313534373032343631350000000042007B01000000B042007A01  
 00000048420069010000002042006A0200000004000000010000000042006B020000000400000000000000004200920900  
 000008000000004B98E05D42000D0200000004000000010000000042000F010000005842005C0500000004000000080000  
 000042007F05000000040000000000000042007C0100000030420094070000002465363936656264302D386562612D34  
 3036652D626532312D64393035396532396261316400000000

Formatted: Font color: Black

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

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
 Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
 Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29ba1d

-----  
42007501000000904200740100000038420067010000002042006802000000400000001000000042006902000000400  
00000000000042008D0200000004000000010000000042000F010000004842005A0500000040000000A00000004200  
760100000030420091070000002434666563336135392D623231372D346162662D383461642D6166313534373032343631  
3500000000  
42007801000000904200770100000038420069010000002042006A02000000400000001000000042006B02000000400  
00000000000042000D0200000004000000010000000042000F010000004842005C0500000040000000A00000004200  
790100000030420094070000002465363936656264302D386562612D343036652D626532312D6439303539653239626131  
6400000000

Formatted: Font color: Black

Out: objectType = '00000002', uuidKey, symmetricKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0782B (Mon Sep 28 10:47:39 CEST 2009)0x000000004B98E05D (Thu Mar 11 13:21:49 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Result Status (0x4200760x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29ba1d  
Tag: Symmetric Key (0x42008E0x42008F), Type: Structure (0x01), Data:  
Tag: Key Block (0x42003E0x420040), Type: Structure (0x01), Data:  
Tag: Key Format Type (0x4200400x420042), Type: Enumeration (0x05), Data: 0x00000001  
Tag: Key Value (0x4200430x420045), Type: Structure (0x01), Data:  
Tag: Key Material (0x4200410x420043), Type: Octet String (0x08), Data: 3D41DF1C5C20E272212D86B762A8C7B4674B32B1A3266DF1253B0F2C4440B0B0  
Tag: Cryptographic Algorithm (0x4200260x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)  
Tag: Cryptographic Length (0x4200280x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

Formatted: Font color: Black

-----  
42007801000001204200770100000048420067010000002042006802000000400000001000000042006902000000400  
00000000000042008F0900000008000000004AC0782B42000D02000000400000001000000042000F01000000C84200  
5A0500000040000000A0000000042007C05000000040000000000000042007901000000A04200550500000040000000  
0200000000420091070000002434666563336135392D623231372D346162662D383461642D616631353437303234363135  
0000000042008E010000005842003E010000005042004005000000400000001000000042004301000000184200410800  
0000193D41DF1C5C20E272212D86B762A8C7B4420026050000004000000030000000420028020000004000000800000  
000042007B010000012042007A0100000048420069010000002042006A02000000400000001000000042006B02000000  
0400000000000000420092090000008000000004B98E05D42000D02000000400000001000000042000F01000000C8  
42005C0500000040000000A0000000042007F05000000400000000000000042007C01000000A042005705000000400  
000020000000420094070000002465363936656264302D386562612D343036652D626532312D64393035396532396261  
31640000000042008F010000005842004001000000504200420500000040000000100000004200450100000018420043

0800000010674B32B1A3266DF1253B0F2C4440B0B04200280500000004000000030000000042002A0200000004000000800000000

9

Client C:

Get usage allocation

In: `uuidKey, UsageLimitsByteCountUsageLimitsCount='500'`

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29ba1d

Tag: Usage Limits Byte Count (0x4200930x420096), Type: BigLong Integer (0x040x03), Data: 01F40x00000000000001F4 (500)

-----  
42007501000000A0420074010000003842006701000000204200680200000004000000010000000042006902000000040000000000000042000B02000000040000000010000000042006A0500000004000000110000000042006B0600000004000000003336135392D623231372D346162662D383461642D6166631353437303234363135000000042009304000000080000000000000001F4

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000001100000000420070100000040420094070000002465363936656264302D386562612D343036652D626532312D6439303539653239626131640000000042009603000000080000000000000001F4

Out: `uuidKeyOperation Failed, Permission Denied`

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:

Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0782B (Mon Sep 28 10:47:39 CEST 2009)0x000000004B98E05D (Thu Mar 11 13:21:49 CET 2010)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)

Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)

Tag: Result Reason (0x42007B0x42007E), Type: Enumeration (0x05), Data: 0x0000000C (Permission Denied)

Tag: Result Message (0x42007A0x42007D), Type: Text String (0x07), Data: Unable to allocate requested byte amount

-----  
42007801000000B8420077010000004842006701000000204200680200000004000000010000000042006902000000040000000000000042000B09000000008000000004AC0782B42000D0200000004000000010000000042000F010000006042005A050000000400000011000000042007C0500000004000000010000000042007B05000000040000000C0000000042007A

Formatted: Font color: Black

Formatted: Font color: Black

0700000028556E61626C6520746F20616C6E6F6361746520726571756573746564206279746520616D6F756E7442007B01  
000000B842007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000  
000000420092090000000800000004B98E05D42000D020000000400000001000000004200F010000006042005C050000  
0004000000110000000042007F0500000004000000010000000042007E05000000040000000C0000000042007D07000000  
23556E61626C6520746F20616C6E6F636174652072657175657374656420616D6F756E740000000000

10 Client A:  
Revoke (symmetric key as cessation of operation) and Destroy (symmetric key)  
In (header): batchOrderOption='TRUE'  
In: uuidKey, revocationReasonCode='6'  
In: uuidKey

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1x00000002 (2))  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 727A212BC674B4EA  
Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29bald

42007501000000904200740100000038420067010000002042006802000000040000000100000000420069020000000400  
0000000000004200690200000004000000010000000042006A0100000004842006B050000000400000001400000004200  
760100000030420091070000002434666563336135292D623231372D346162662D383461642D61666313534373032343631  
3500000000

Out: uuidKey

Tag: Response Message (0x420078), Type: Structure (0x01), Data:  
Tag: Response Header (0x420077Revocation Reason (0x420081), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420067Revocation Reason Code (0x420082), Type: Structure (0x01)Enumeration (0x05), Data:  
Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x42008F), Type: Date-Time (0x09), Data: 0x000000004AC0782C (Mon Sep 28 10:47:40 CEST 2009)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1x00000006 (Cessation of Operation))  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Result Status (0x42007CUnique Batch Item ID (0x420093), Type: Enumeration (0x05)Octet String (0x08), Data: 0x00000000 (Success)ID0EBF826109B0A5  
Tag: ResponseRequest Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: 4fee3a59-b217-4abf-84ad-af1547024615e696ebd0-8eba-406e-be21-d9059e29bald

42007801000000B04200770100000048420067010000002042006802000000040000000100000000420069020000000400

Formatted: Font color: Black

00000000000042008F09000000000000004AC9782C42000D020000004000000010000000042000F01000000584200  
5A950000000400000014000000042007C050000000400000000000000042007901000000304200910700000024346665  
63336135392D623231372D346162662D383461642D6166313534373032343631350000000420078010000012842007701  
00000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200100600  
00000800000000000000142000D0200000004000000020000000042000F010000007042005C0500000004000000130000  
00004200930800000008727A212BC674B4EA4200790100000048420094070000002465363936656264302D386562612D34  
3036652D626532312D643930353965323962613164000000042008101000000104200820500000040000000600000000  
42000F010000005842005C050000000400000014000000042009308000000081D0EBF826109B0A5420079010000003042  
0094070000002465363936656264302D386562612D343036652D626532312D64393035396532396261316400000000

[Out: uuidKey](#)

[Out: uuidKey](#)

[Tag: Response Message \(0x42007B\), Type: Structure \(0x01\), Data:](#)

[Tag: Response Header \(0x42007A\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version \(0x420069\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version Major \(0x42006A\), Type: Integer \(0x02\), Data: 0x00000001 \(1\)](#)

[Tag: Protocol Version Minor \(0x42006B\), Type: Integer \(0x02\), Data: 0x00000000 \(0\)](#)

[Tag: Time Stamp \(0x420092\), Type: Date-Time \(0x09\), Data: 0x00000004B98E05F \(Thu Mar 11 13:21:51 CET 2010\)](#)

[Tag: Batch Count \(0x42000D\), Type: Integer \(0x02\), Data: 0x00000002 \(2\)](#)

[Tag: Batch Item \(0x42000F\), Type: Structure \(0x01\), Data:](#)

[Tag: Operation \(0x42005C\), Type: Enumeration \(0x05\), Data: 0x00000013 \(Revoke\)](#)

[Tag: Unique Batch Item ID \(0x420093\), Type: Octet String \(0x08\), Data: 727A212BC674B4EA](#)

[Tag: Result Status \(0x42007F\), Type: Enumeration \(0x05\), Data: 0x00000000 \(Success\)](#)

[Tag: Response Payload \(0x42007C\), Type: Structure \(0x01\), Data:](#)

[Tag: Unique Identifier \(0x420094\), Type: Text String \(0x07\), Data: e696ebd0-8eba-406e-be21-d9059e29bald](#)

[Tag: Batch Item \(0x42000F\), Type: Structure \(0x01\), Data:](#)

[Tag: Operation \(0x42005C\), Type: Enumeration \(0x05\), Data: 0x00000014 \(Destroy\)](#)

[Tag: Unique Batch Item ID \(0x420093\), Type: Octet String \(0x08\), Data: 1D0EBF826109B0A5](#)

[Tag: Result Status \(0x42007F\), Type: Enumeration \(0x05\), Data: 0x00000000 \(Success\)](#)

[Tag: Response Payload \(0x42007C\), Type: Structure \(0x01\), Data:](#)

[Tag: Unique Identifier \(0x420094\), Type: Text String \(0x07\), Data: e696ebd0-8eba-406e-be21-d9059e29bald](#)

42007B010000013042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400  
000000000000420092090000000800000004B98E05F42000D0200000004000000020000000042000F01000000684200  
5C050000000400000013000000004200930800000008727A212BC674B4EA42007F0500000004000000000000042007C  
0100000030420094070000002465363936656264302D386562612D343036652D626532312D643930353965323962613164  
0000000042000F010000006842005C050000000400000014000000042009308000000081D0EBF826109B0A542007F0500  
0000040000000000000042007C0100000030420094070000002465363936656264302D386562612D343036652D626532  
312D64393035396532396261316400000000

138  
139

## 66 Key Interchange, Key Exchange

140

### 6.16.1 Use-case: Import of a Third-party Key

142  
143

**Formatted:** Style Heading 1h1Level 1 Topic  
Heading + Before: 5 pt After: 5..., Outline  
numbered + Level: 1 + Numbering Style: 1, 2,  
3, ... + Start at: 3 + Alignment: Left + Aligned  
at: 0 pt + Indent at: 0 pt

**Formatted:** Indent: Left: 0 pt, Outline  
numbered + Level: 2 + Numbering Style: 1, 2,  
3, ... + Start at: 1 + Alignment: Left + Aligned  
at: 36 pt + Indent at: 36 pt, Don't adjust  
space between Latin and Asian text

**Formatted:** Font: Not Bold



144 This use-case tests the import of a foreign key using the Register operation. To validate that the  
 145 registered key is treated the same as a locally created key, an attribute is added to the key and then  
 146 modified. Finally, the key is destroyed.  
 147

Time	Request/Response messages
0	<p>Register (symmetric key)            In: objectType = '00000002', attributes={ CryptographicUsageMask='00000004' }, foreignSymmetricKey</p> <p>Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:            Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:              Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:                Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)                Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)              Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)              Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:                Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)                Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:                  Tag: Object Type (0x4200550x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)                  Tag: Template-Attribute (0x42008E0x420091), 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 (0x42008E0x42008F), Type: Structure (0x01), Data:                      Tag: Key Block (0x42003E0x420040), Type: Structure (0x01), Data:                        Tag: Key Format Type (0x4200490x420042), Type: Enumeration (0x05), Data: 0x00000001                        Tag: Key Value (0x4200430x420045), Type: Structure (0x01), Data:                          Tag: Key Material (0x4200410x420043), Type: Octet String (0x08), Data:                          0123456789ABCDEF0123456789ABCDEF                          Tag: Cryptographic Algorithm (0x4200260x420028), Type: Enumeration (0x05), Data:                          0x00000003 (AES)                          Tag: Cryptographic Length (0x4200290x42002A), Type: Integer (0x02), Data: 0x00000080 (128)                          4200750100000110420074010000003842006701000000204200680200000004000000010000000042006902000000040                          000000000000004200000200000004000000010000000042000F01000000C842005A0500000004000000030000000042                          007601000000B04200550500000004000000020000000042008E0100000038420008010000003042000A0700000018437                          27970746F67726170686963205573616765204D61736B42000B020000000400000004000000042008C01000000584200                          3E010000005042004005000000040000000100000000420043010000001842004108000000100123456789ABCDEF01234                          56789ABCDEF4200260500000004000000030000000042002802000000040000008000000000                          42007801000001104200770100000038420069010000002042006A0200000004000000010000000042006B02000000040                          000000000000004200000200000004000000010000000042000F01000000C842005C0500000004000000030000000042                          007901000000B0420057050000000400000002000000004200910100000038420008010000003042000A0700000018437                          27970746F67726170686963205573616765204D61736B42000B020000000400000004000000042008F01000000584200                          40010000005042004205000000040000000100000000420045010000001842004308000000100123456789ABCDEF01234                          56789ABCDEF4200280500000004000000030000000042002A02000000040000008000000000</p> <p>Out: uuidKey</p> <p>Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:            Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:</p>

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
 Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0782C (Mon Sep 28 0x000000004AFBED32 (Thu Nov 12 12:10:47-40-CEST42 CET 2009))  
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
 Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)  
 Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
 Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:  
 Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: bb806453-5e75-42e2-80bd-4e52f1eeb57b6e1a5a83-8113-4260-b40d-966f231b91b7

4200780100000000042007701000000048420067010000002042006802000000040000000100000000420069020000000400000000000042008F01000000005842005A05000000040000000000000042007C050000000400000000000000004200790100000030420091070000002462623820363435332D356337352D34326332D383062642D3465353266316365623537620000000042007B010000000042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED3242000D0200000004000000010000000042000F010000005842005C0500000004000000030000000042007F0500000004000000000000000042007C0100000030420094070000002436653161356138332D383131332D343236302D623430642D39363666323331623931623700000000

1 Add attribute  
 In: uuidKey, attribute={ x-provider='unknown' }

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:  
 Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:  
 Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:  
 Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
 Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)  
 Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:  
 Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: bb806453-5e75-42e2-80bd-4e52f1eeb57b6e1a5a83-8113-4260-b40d-966f231b91b7  
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-provider  
 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: unknown

420075010000000004200740100000003842006701000000204200680200000004000000010000000042006902000000040000000000000042008F01000000007842005A0500000004000000000000000042007C050000000400000000000000004200790100000030420091070000002462623830363435332D356337352D34326332D383062642D3465353266316365623537620000000042008010000002842000A070000000A782D70726F766964657200000000000042000B0700000007756E6B6E6F776E00

420078010000000004200770100000038420067010000002042006A0200000004000000010000000042006B02000000040000000000000042000F010000007842005C050000000400000000000000004200790100000060420094070000002436653161356138332D383131332D343236302D623430642D3936366632333162393162370000000042008010000002842000A070000000A782D70726F766964657200000000000042000B0700000007756E6B6E6F776E00

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

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:

Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC0782E (Mon Sep 28 0x000000004AFBED32 (Thu Nov 12 12:10:47+42 GMT CET 2009))

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)

Tag: Result Status (0x4200760x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: bb806453-5e75-42e2-80bd-4e52f1eeb57b6e1a5a83-8113-4260-b40d-966f231b91b7

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

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

Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: unknown

4200780100000000042007701000000048420067010000002042006802000000400000001000000004200690200000004000000000000042008F0900000000800000004AC0782E42000D020000004000000010000000042000F010000008842005A05000000040000000000000042007C050000000400000000000000004200790100000060420091070000002462623830363435332D356337352D343263322D383062642D346535326631636562353762000000042008010000002842000A07000000A782B70726F76696465720000000000042000B0700000007756E6B6E6F776E0042007B01000000E042007A0100000048420069010000002042006A020000004000000010000000042006B020000004000000000000000420092090000008000000004AFBED3242000D02000000400000001000000042000F010000008842005C050000000400000000D000000042007F05000000040000000000000042007C0100000060420094070000002436653161356138332D383131332D34326302D623430642D3936366323316239316237000000042008010000002842000A07000000A782B70726F76696465720000000000042000B0700000007756E6B6E6F776E00

2

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

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: bb806453-5e75-42e2-80bd-4e52f1eeb57b6e1a5a83-8113-4260-b40d-966f231b91b7

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

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

Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: third party

4200750100000000C84200740100000038420067010000002042006802000000400000001000000004200690200000004000000000000042008F0900000000800000004AC0782E42000D020000004000000010000000042000F010000008842005A05000000040000000000000042007C050000000400000000000000004200790100000060420091070000002462623830363435332D356337352D343263322D383062642D346535326631636562353762000000042008010000002842000A07000000A782B70726F76696465720000000000042000B0700000007756E6B6E6F776E0042007B01000000E042007A0100000048420069010000002042006A020000004000000010000000042006B020000004000000000000000420092090000008000000004AFBED3242000D02000000400000001000000042000F010000008842005C050000000400000000D000000042007F05000000040000000000000042007C0100000060420094070000002436653161356138332D383131332D34326302D623430642D3936366323316239316237000000042008010000002842000A07000000A782B70726F76696465720000000000042000B0700000007756E6B6E6F776E00

4200780100000000C84200770100000038420069010000002042006A020000004000000010000000042006B020000004000000000000000420092090000008000000004AFBED3242000D02000000400000001000000042000F010000008842005C050000000400000000D000000042007F05000000040000000000000042007C0100000060420094070000002436653161356138332D383131332D34326302D623430642D3936366323316239316237000000042008010000002842000A07000000A782B70726F76696465720000000000042000B0700000007756E6B6E6F776E00

6972642070617274790000000000

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

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:

Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x000000004AC0782E (Mon Sep 28 0x000000004AFBED32 (Thu Nov 12 12:10:47:42 CEST CET 2009))

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)

Tag: Result Status (0x42007E0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: bb806453-5e75-42e2-80bd-4e52f1eeb57b6e1a5a83-8113-4260-b40d-966f231b91b7

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

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

Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: third party

42007801000000E84200770100000048420067010000002042006802000000040000000100000000420069020000000400000000000042008F0900000008000000004AC0782E42000D0200000004000000010000000042000F010000009042005A0500000040000000E0000000042007C050000000400000000000000004200790100000068420091070000002462623830363435332D3326337352D34326332D383062642D3465353266316365623537620000000420008010000003042000A070000000A782D70726F76696465720000000000042000B070000000B746869726420706172747900000000042007B01000000E842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED3242000D0200000004000000010000000042000F010000009042005C0500000040000000E0000000042007F0500000004000000000000000042007C0100000068420094070000002436653161356138332D383131332D343263302D623430642D3936366632333162393162370000000420008010000003042000A07000000A782D70726F76696465720000000000042000B070000000B74686972642070617274790000000000

3

Destroy (symmetric key)

In: uuidKey

Tag: Request Message (0x4200750x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x4200740x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

Tag: Request Payload (0x4200760x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: bb806453-5e75-42e2-80bd-4e52f1eeb57b6e1a5a83-8113-4260-b40d-966f231b91b7

4200750100000090420074010000003842006701000000204200680200000004000000010000000042006902000000040000000000004200740100000000420077050000000400000000000000004200780100000068420091070000002462623830363435332D3326337352D34326332D383062642D34653532663163656235376200000000420008010000003042000A070000000A782D70726F76696465720000000000042000B070000000B746869726420706172747900000000042007901000000009042005C0500000040000000E0000000042007F0500000004000000000000000042007C0100000068420094070000002436653161356138332D383131332D343263302D623430642D3936366632333162393162370000000420008010000003042000A07000000A782D70726F76696465720000000000042000B070000000B74686972642070617274790000000000

0000000000004200D020000004000000100000004200F01000004842005C050000004000001400000004200790100000030420094070000002436653161356138332D383131332D343236302D623430642D39363666323331623931623700000000

Out: uuidKey

Tag: Response Message (0x4200780x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x4200770x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x4200670x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x4200680x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x4200690x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x42008F0x420092), Type: Date-Time (0x09), Data: 0x00000004AC0782E (Mon Sep 28 0x000000004AFBED32 (Thu Nov 12 12:10:47+42 CESTCET 2009)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005A0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
Tag: Result Status (0x42007C0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x4200790x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x4200910x420094), Type: Text String (0x07), Data: bb806453-5e75-42e2-80bd-4e52f1eeb57b61a5a83-8113-4260-b40d-966f231b91b7

42007801000000B04200770100000048420067010000002042006802000000040000000100000000420069020000000400000000000042008F0900000008000000004AC0782E42000D0200000004000000010000000042009010000005842005A0500000004000000140000000042007C050000000400000000000000004200790100000030420091070000002462623830363435332D356337352D343263322D383062642D3465353266316365623537620000000042007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000004200920900000008000000004AFBED3242000D020000000400000001000000042000F010000005842005C050000004000000140000000042007F05000000040000000000000042007C0100000030420094070000002436653161356138332D383131332D343236302D623430642D39363666323331623931623700000000

148
149
150
151
152
153
154
155
156
157
158
159

## 77 Vendor Extensions

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

### 7.47.1 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.

Formatted: Style Heading 1h1Level 1 Topic Heading + Before: 5 pt After: 5..., Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 3 + Alignment: Left + Aligned at: 0 pt + Indent at: 0 pt

Formatted: Indent: Left: 0 pt, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 36 pt + Indent at: 36 pt, Don't adjust space between Latin and Asian text

Formatted: Font: Not Bold

Time	Client A
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C' }, MessageExtension={ VendorIdentification='Acme', CriticalityIndicator='false', VendorExtension={ tag='0x540001', type='text string', value='na' } }

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
    Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
      Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
        Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
        Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:  
          Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
            Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length  
            Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)  
          Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
            Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm  
            Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)  
          Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
            Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage  
Mask  
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt,  
Decrypt)  
    Tag: Message Extension (0x420051), Type: Structure (0x01), Data:  
      Tag: Criticality Indicator (0x420026), Type: Boolean (0x06), Data: FALSE  
      Tag: Vendor Identification (0x42009D), Type: Text String (0x07), Data: Acme  
    Tag: Vendor Extension (0x42009C), Type: Structure (0x01), Data:  
      Tag: Unknown tag (0x014242), Type: Text String (0x07), Data: na

420078010000001604200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000011842005C05000000040000000100000000420079010000000C04200570500000004000000020000000042009101000000A8420008010000003042000A070000001443727970746F67726170686963204C656E677468000000042000B02000000040000000800000000420008010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000040000000C000000000420051010000003842002606000000080000000000000042009D070000000441636D65000000042009C010000001001424207000000026E61000000000000

Out: objectType='00000002', uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73BF1C (Thu Feb 11 09:26:04 CET 2010)  
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
    Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
      Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
      Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
        Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 052eff73-b35e-4702-9db9-37c12f0151d3

42007B010000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000420092090000008000000004B73BF1C4200D0200000040000000100000004200F010000006842005C05000000400000010000000042007F05000000040000000000000042007C010000004042005705000000040000200000000420094070000002430353265666637332D623335652D343730322D396462392D33376331326630313531643300000000

Formatted: Font: Courier New, 8 pt, Font color: Black

1 Destroy (symmetric key)  
In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 052eff73-b35e-4702-9db9-37c12f0151d3

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000420092090000008000000004B73BF1C4200D0200000040000000100000004200F010000004842005C050000000400000014000000004200790100000030420094070000002430353265666637332D623335652D343730322D396462392D33376331326630313531643300000000

Out: uuidKey

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000420092090000008000000004B73BF1C4200D0200000040000000100000004200F010000005842005C0500000004000000140000000042007F05000000040000000000000042007C0100000030420094070000002430353265666637332D623335652D343730322D396462392D33376331326630313531643300000000

Formatted: Font: Courier New, 8 pt, Font color: Black

160  
161

162  
163  
164  
165  
166  
167

## 7.27.2 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.

Formatted: Indent: Left: 0 pt, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 36 pt + Indent at: 36 pt, Don't adjust space between Latin and Asian text  
Formatted: Font: Not Bold

Time	Client A
0	<p>Create (symmetric key)</p> <p>In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C' }, MessageExtension={ VendorIdentification='Acme', CriticalityIndicator='true', VendorExtension={ tag='0x540001', type='text string', value='na' } }</p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</u></p> <p><u>Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)</u></p> <p><u>Tag: Message Extension (0x420051), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Criticality Indicator (0x420026), Type: Boolean (0x06), Data: TRUE</u></p> <p><u>Tag: Vendor Identification (0x42009D), Type: Text String (0x07), Data: Acme</u></p> <p><u>Tag: Vendor Extension (0x42009C), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unknown tag (0x014242), Type: Text String (0x07), Data: na</u></p> <p>42007801000001604200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000042000D020000004000000010000000042000F010000011842005C0500000004000000010000000042007901000000C0420057050000000400000002000000042009101000000A8420008010000003042000A070000001443727970746F67726170686963204C656E677468000000042000B020000000400000008000000000420008010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000040000000C00000000420051010000003842002606000000080000000000000142009D070000000441636D65000000042009C01000001001424207000000026E61000000000000</p>



Out: Operation Failed, Feature Not Supported

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

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B73BF1D42000D0200000004000000010000000042000F010000006842005C0500000004000000010000000042007F0500000004000000010000000042007E0500000004000000080000000042007D0700000029437269746963616C204D65737361676520457874656E73696F6E206E6F74207265636F676E697A6564000000000000

168  
169  
170  
171  
172  
173  
174  
175  
176  
177

## 88 Asymmetric keys

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

### 8.18.1 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.

Formatted: Style Heading 1h1Level 1 Topic Heading + Before: 5 pt After: 5..., Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 3 + Alignment: Left + Aligned at: 0 pt + Indent at: 0 pt

Formatted: Indent: Left: 0 pt, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 36 pt + Indent at: 36 pt, Don't adjust space between Latin and Asian text

Formatted: Font: Not Bold

Time	Client A
0	Create Key Pair In: commonAttributes={ CryptographicAlgorithm='RSA', CryptographicLength='1024', <u>CryptographicUsageMask='0000000C'</u> }, privateKeyAttributes={ Name={ NameValue='PrivateKey1', NameType='00000001' }}, <u>CryptographicUsageMask='00000001'</u> }, publicKeyAttributes={ NameValue='PublicKey1', NameType='00000001' }}, <u>CryptographicUsageMask='00000002'</u> }  Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000002 (Create Key Pair)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Common Template-Attribute (0x42001F), Type: Structure (0x01), Data:  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm  
Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (RSA)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length  
Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000400 (1024)  
Tag: Private Key Template-Attribute (0x420065), Type: Structure (0x01), Data:  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name  
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:  
Tag: Name Value (0x420055), Type: Text String (0x07), Data: PrivateKey1  
Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage  
Mask  
Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000001 (Sign)  
Tag: Public Key Template-Attribute (0x42006E), Type: Structure (0x01), Data:  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name  
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:  
Tag: Name Value (0x420055), Type: Text String (0x07), Data: PublicKey1  
Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage  
Mask  
Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000002 (Verify)  
  
42007801000001E84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040  
000000000000042000D020000004000000010000000042000F01000001A042005C0500000004000000020000000042  
0079010000018842001F0100000070420008010000003042000A070000001743727970746F6772617068696320416C676  
F726974686D0042000B0500000004000000040000000420008010000003042000A070000001443727970746F67726170  
686963204C65E677468000000042000B020000000400000040000000004200650100000080420008010000004042000  
A07000000044E616D65000000042000B0100000028420055070000000B507269766174654B657931000000000420054  
0500000004000000010000000420008010000003042000A070000001843727970746F677261706869632055736167652  
04D61736B42000B0200000004000000010000000042006E0100000080420008010000004042000A07000000044E616D65  
0000000042000B0100000028420055070000000A5075626C69634B657931000000000004200540500000004000000010  
0000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200  
0000040000000200000000

**Out: uuidPrivateKey, uuidPublicKey**

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

	<p><a href="#">Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13A (Thu Feb 11 09:35:06 CET 2010)</a></p> <p><a href="#">Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</a></p> <p><a href="#">Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000002 (Create Key Pair)</a></p> <p><a href="#">Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</a></p> <p><a href="#">Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-6dc2115cc042</a></p> <p><a href="#">Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-879bab490259</a></p> <p>42007B010000000E042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B73C13A42000D02000000400000001000000042000F010000008842005C0500000004000000020000000042007F05000000040000000000000042007C0100000060420094070000002438393566373263322D623230612D343964382D393530342D3664633231313563633034320000000420094070000002461323432666361342D656266302D343339382D616336352D38373962616234393032353900000000</p>
1	<p>Locate (Public Key)</p> <p>In: attributes={ objectType='PublicKey', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey }}</p> <p><a href="#">Tag: Request Message (0x420078), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Request Header (0x420077), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</a></p> <p><a href="#">Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</a></p> <p><a href="#">Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</a></p> <p><a href="#">Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)</a></p> <p><a href="#">Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Attribute (0x420008), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type</a></p> <p><a href="#">Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (Public Key)</a></p> <p><a href="#">Tag: Attribute (0x420008), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link</a></p> <p><a href="#">Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000103 (Private Key Link)</a></p> <p><a href="#">Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-879bab490259</a></p> <p>420078010000000F04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F01000000A842005C050000000400000008000000004200790100000090420008010000002842000A070000000B4F626A656374205479706500000000042000B05000000040000000000000420008010000005842000A07000000044C696E6B000000042000B010000004042004B0500000004000001030000000042004C070000002461323432666361342D656266302D343339382D616336352D38373962616234393032353900000000</p> <p>Out: uuidPublicKey</p> <p><a href="#">Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</a></p>

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13B (Thu Feb 11 09:35:07 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-6dc2115cc042  
  
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B73C13B42000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F05000000040000000000000042007C0100000030420094070000002438393566373263322D623230612D343964382D393530342D36646332313135636330343200000000

2  
Locate (Private Key)  
In: attributes={ objectType='PrivateKey', Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey }}  
  
Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type  
Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Private Key)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link  
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:  
Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000102 (Public Key Link)  
Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-6dc2115cc042  
  
42007801000000F04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F01000000A842005C0500000004000000080000000004200790100000090420008010000002842000A070000000B4F626A656374205479706500000000042000B050000000400000000040000000420008010000005842000A07000000044C696E6B0000000042000B0100000004042004B0500000004000001020000000042004C070000002438393566373263322D623230612D343964382D393530342D36646332313135636330343200000000

Out: uuidPrivateKey  
  
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13B (Thu Feb 11 09:35:07 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-879bab490259  
  
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B73C13B42000D020000004000000010000000042000F010000005842005C050000004000000080000000042007F0500000040000000000000042007C0100000030420094070000002461323432666361342D656266302D343339382D616336352D38373962616234393032353900000000

3  
**Destroy**  
**In: uuidPrivateKey**

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-879bab490259  
  
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002461323432666361342D656266302D343339382D616336352D38373962616234393032353900000000

**Out: uuidPrivateKey**

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

	<p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-879bab490259</u></p> <p><u>42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000042009209000000800000004B73C13B42000D020000004000000010000000042000F010000005842005C050000004000000140000000042007F05000000040000000000000042007C0100000030420094070000002461323432666361342D656266302D343339382D616336352D38373962616234393032353900000000</u></p>
4	<p><b>Destroy</b></p> <p><b>In: uuidPublicKey</b></p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-6dc2115cc042</u></p> <p><u>42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042009209000000800000004B73C13B42000D020000004000000010000000042000F010000005842005C050000004000000140000000042007F05000000040000000000000042007C0100000030420094070000002438393566373263322D623230612D343964382D393530342D36646332313135636330343200000000</u></p> <p><b>Out: uuidPublicKey</b></p> <p><u>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13B (Thu Feb 11 09:35:07 CET 2010)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</u></p> <p><u>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</u></p> <p><u>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-6dc2115cc042</u></p> <p><u>42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000042009209000000800000004B73C13B42000D020000004000000010000000042000F010000005842005C050000004000000140000000042007F05000000040000000000000042007C0100000030420094070000002438393566373263322D623230612D343964382D393530342D36646332313135636330343200000000</u></p>

179 **8.28.2 Use-case: Register Both Halves of a Key Pair**

180 Register a private key and a public key and set the Link attribute to point to each other. Verify the links  
181 were set correctly by locating the keys based on the link attributes, and then delete both objects.  
182

Formatted: Indent: Left: 0 pt, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 36 pt + Indent at: 36 pt, Don't adjust space between Latin and Asian text  
Formatted: Font: Not Bold

Time	Client A
0	<p>Register (Private Key)</p> <p>In: objectType='00000004', attributes={ CryptographicUsageMask='0000000C<u>00000001</u>' }, foreignPrivateKey</p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000004 (Private Key)</u></p> <p><u>Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000001 (Sign)</u></p> <p><u>Tag: Private Key (0x420064), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Key Block (0x420040), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000004</u></p> <p><u>Tag: Key Value (0x420045), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Key Material (0x420043), Type: Octet String (0x08), Data:</u>  30820276020100300D06092A864886F70D0101010500048202603082025C02010002818100930451C9ECD94F5BB9DA17D  D09381BD23BE43ECA8C7539F301FC8A8CD5D5274C3E7699DBDC711C97A7AA91E2C50A82BD0B1034F0DF493DEC16362427  E58ACCE7F6CE0F9BCC617BBD8C90D0094A2703BA0D09EB19D1005F2FB265526AAC75AF32F8BC782CDED2A57F811E03EAF  67A944DE5E78413DCA8F232D074E6DCEAA4CE9F02030100010281800B6A7D736199EA48A420E4537CA0C7C046784DCBEA  A63BAEBC0BC132787449CDE8D7CAD0C0C863C0FEFB06C3062BEFC50033ECF87B4E33A9BE7BCBC8F1511AE215E80DEB5D8  AF2BD31319D7821196640935A0CD67C94599579F2100D65E038831FDAFB0DBE2BBDAC00A696E67E756350E1C99ACE11A3  6DABAC3ED3E730960059024100DDF672FBCC5BDA3D73AFFC4E791E0C03390224405D69CCAABC749FAA0DCD4C2583C71DD  E8941A7B9AA030F52EF1451466C074D4D338FE677892ACD9E10FD35BD024100A98FBC3ED6B4C6F860F97165AC2F7BB6F2  E2CB192A9ABD49795BE5BCF37D8EE69A6E169C24E5C32E4E7FA33265461407F952BA49E20481A2F785F113F922B8B024  0253F9470390D39049303777DDBC9750E9D64849CE0903EAE704DC9F589B7680DEB9D609FD5BCD4DEC6F120542E5CF5  D76F2A43C8615FB5B3A9213463797AA9024100A1DDDF023C0CD94C019BB26D09B9E3CA8FA971CB16AA58B9BAF79D6081A1  DBBA452BA53653E2804BA98FF69E8BB1B3A161EA225EA501463216A8DAB9B88A75E5F02406178646E112CF79D921A8A84  3F17F6E7FF974F688122365BF6690CDFC996E1890952EB3820DD1890EC1C8619E87A2BD38F9D03B37FAC742EFB748C788  5942C39</p> <p><u>Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000004</u>  (RSA)</p> <p><u>Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000400 (1024)</u></p> <p>42007801000003804200770100000038420069010000002042006A020000000400000001000000042006B0200000040  000000000000042000D0200000040000000100000004200F010000033842005C050000004000000030000000042  007901000003204200570500000040000000400000004200910100000038420008010000003042000A0700000018437  27970746F7726170686963205573616765204D61736B42000B02000000400000001000000042006401000002C84200  4001000002C04200420500000040000000400000004200450100000288420043080000027A30820276020100300D060  92A864886F70D0101010500048202603082025C02010002818100930451C9ECD94F5BB9DA17DD09381BD23BE43ECA8C75  39F301FC8A8CD5D5274C3E7699DBDC711C97A7AA91E2C50A82BD0B1034F0DF493DEC16362427E58ACCE7F6CE0F9BCC617</p>

BBD8C9D0094A2703BA0D09EB19D1005F2FB265526AAC75AF32F8BC782CDED2A57F811E03EAF67A944DE5E78413DCA8F232D074E6DC9A4CECF9F02030100010281800B6A7D736199EA48A420E4537CA0C7C046784DCBAA63BAEBC0BC132787449CDE8D7CAD0C0C863C0FEF806C3062BEFC50033ECF87B4E33A9BE7BCBC8F1511AE215E80DEB5D8AF2BD31319D7821196640935A0CD67C94599579F2100D65E038831FDAFB0DBE2BBDAC00A696E67E756350E1C99ACE11A36DABAC3ED3E730960059024100DDF672FBCC5BDA3D73AFFC4E791E0C03390224405D69CCAABC749FAA0DCD4C2583C71DDE8941A7B9AA030F52EF1451466C074D4D338FE677892ACD9E10FD35BD024100A98FBC3ED6B4C6F860F97165AC2F7BB6F2E2CB192A9ABD49795BE5B CF37D8EE69A6E169C24E5C32E4E7FA33265461407F952BA49E204818A2F785F113F922B8B0240253F9470390D39049303777DDBC9750E9D64849CE0903EAE704DC9F589B7680DEB9D609FD5BCD4DECD6F120542E5CFF5D76F2A43C8615FB5B3A9213463797AA9024100A1DDF023C0CD94C019BB26D09B9E3CA8FA971CB16AA58B9BAF79D6081A1DDBA452BA53653E2804BA98FF69E8BB1B3A161EA225EA501463216A8DAB9B88A75E5F02406178646E112CF79D921A8A843F17F6E7FF974F688122365BF690CDFC996E1890952EB3820DD1890EC1C8619E87A2BD38F9D03B37FAC742EFB748C7885942C390000000000042002805000000400000004000000042002A020000004000004000000000

Out: uuidPrivateKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A1 (Thu Feb 11 09:49:37 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66d27b11943

42007B010000000042007A01000000048420069010000002042006A020000000400000001000000042006B0200000004000000000000420092090000000800000004B73C4A142000D0200000040000000100000004200F010000005842005C050000004000000030000000042007F05000000040000000000000042007C0100000030420094070000002466613036303638632D366662312D343265612D623661322D64363664323762313139343300000000

1 Register (Public Key)

In: objectType='00000004', attributes={ CryptographicUsageMask='0000000C'00000002', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey }}, foreignPublicKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)

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

Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000003 (Public Key)

Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:

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

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

Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000002 (Verify)



Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link  
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:  
Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000103 (Private Key Link)  
Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: fa06068c-6fbl-42ea-b6a2-d66d27b11943  
Tag: Public Key (0x42006D), Type: Structure (0x01), Data:  
Tag: Key Block (0x420040), Type: Structure (0x01), Data:  
Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000005  
Tag: Key Value (0x420045), Type: Structure (0x01), Data:  
Tag: Key Material (0x420043), Type: Octet String (0x08), Data:  
30819F300D06092A864886F70D0101050003818D0030818902818100930451C9ECD94F5BB9DA17DD09381BD23BE43EC  
A8C7539F301FC8A8CD5D5274C3E7699DBDC711C97A7AA91E2C50A82BD0B1034F0DF493DEC16362427E58ACCE7F6CE0F9B  
CC617BBD8C90D0094A2703BA0D09EB19D1005F2FB265526AAC75AF32F8BC782CDED2A57F811E03EAF67A944DE5E78413D  
CA8F232D074E6DCEA4CEC9F0203010001  
Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000004 (RSA)  
Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000400 (1024)

```

42007801000002084200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000042000D020000004000000010000000042000F01000001C042005C050000004000000030000000042
007901000001A842005705000000040000000300000004200910100000098420008010000003042000A0700000018437
27970746F7726170686963205573616765204D61736B42000B0200000004000000020000000042000801000000584200
0A07000000044C696E6B000000042000B010000004042004B050000000400000103000000042004C070000002466613
036303638632D366662312D343265612D623661322D643636643237623131393433000000042006D01000000F0420040
01000000E8420042050000000400000005000000042004501000000B04200430800000A230819F300D06092A864886F
70D010101050003818D0030818902818100930451C9ECD94F5BB9DA17DD09381BD23BE43ECA8C7539F301FC8A8CD5D527
4C3E7699DBDC711C97A7AA91E2C50A82BD0B1034F0DF493DEC16362427E58ACCE7F6CE0F9BCC617BBD8C90D0094A2703B
A0D09EB19D1005F2FB265526AAC75AF32F8BC782CDED2A57F811E03EAF67A944DE5E78413DCA8F232D074E6DCEA4CEC9F
02030100010000000000042002805000000400000004000000042002A02000000040000040000000000

```

Out: uuidPublicKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B73C4A2 (Thu Feb 11 09:49:38 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 79cbf228-16df-4fbl-a385-443546935e74

```

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000420092090000000800000004B73C4A242000D0200000004000000010000000042000F010000005842
005C050000000400000003000000042007F050000000400000000000000042007C01000000304200940700000024373
96362663232382D313664662D346662312D613338352D34343335343639333565373400000000

```

2 Add attribute  
In: uuidPrivateKey, attribute={ Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } }

[Tag: Request Message \(0x420078\), Type: Structure \(0x01\), Data:](#)  
[Tag: Request Header \(0x420077\), Type: Structure \(0x01\), Data:](#)  
[Tag: Protocol Version \(0x420069\), Type: Structure \(0x01\), Data:](#)  
[Tag: Protocol Version Major \(0x42006A\), Type: Integer \(0x02\), Data: 0x00000001 \(1\)](#)  
[Tag: Protocol Version Minor \(0x42006B\), Type: Integer \(0x02\), Data: 0x00000000 \(0\)](#)  
[Tag: Batch Count \(0x42000D\), Type: Integer \(0x02\), Data: 0x00000001 \(1\)](#)  
[Tag: Batch Item \(0x42000F\), Type: Structure \(0x01\), Data:](#)  
[Tag: Operation \(0x42005C\), Type: Enumeration \(0x05\), Data: 0x0000000D \(Add Attribute\)](#)  
[Tag: Request Payload \(0x420079\), Type: Structure \(0x01\), Data:](#)  
[Tag: Unique Identifier \(0x420094\), Type: Text String \(0x07\), Data: fa06068c-6fb1-42ea-b6a2-d66d27b11943](#)  
[Tag: Attribute \(0x420008\), Type: Structure \(0x01\), Data:](#)  
[Tag: Attribute Name \(0x42000A\), Type: Text String \(0x07\), Data: Link](#)  
[Tag: Attribute Value \(0x42000B\), Type: Structure \(0x01\), Data:](#)  
[Tag: Link Type \(0x42004B\), Type: Enumeration \(0x05\), Data: 0x00000102 \(Public Key Link\)](#)  
[Tag: Linked Object Identifier \(0x42004C\), Type: Text String \(0x07\), Data: 79cbf228-16df-4fb1-a385-443546935e74](#)

[42007801000000F04200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000000042000D0200000004000000010000000042000F01000000A842005C050000000400000000D000000004200790100000090420094070000002466613036303638632D366662312D343265612D623661322D64363664323762313139343300000000420008010000005842000A07000000044C696E6B0000000042000B010000004042004B050000000400000102000000042004C070000002437396362663232382D313664662D346662312D613338352D34343335343639333565373400000000](#)

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

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

Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: 79cbf228-16df-4fbl-a385-443546935e74

42007B010000011042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000042009209000000800000004B73C4A24200D0200000040000000100000004200F01000000B842005C0500000040000000D000000042007F05000000040000000000000042007C0100000090420094070000002466613036303638632D343265612D623661322D6436366432376231313934330000000420008010000005842000A07000000044C696E6B000000042000B010000004042004B050000000400000102000000042004C070000002437396362663232382D313664662D346662312D613338352D34343335343639333565373400000000

3

Locate (Public Key)

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

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

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

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

Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (Public Key)

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

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

Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:

Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000103 (Private Key Link)

Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: fa06068c-6fbl-42ea-b6a2-d66d27b11943

42007801000000F04200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000042000D020000000400000001000000004200F01000000A842005C050000000400000008000000004200790100000090420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000300000000420008010000005842000A07000000044C696E6B000000042000B010000004042004B050000000400000103000000042004C070000002466613036303638632D343265612D623661322D64363664323762313139343300000000

Out: uuidPublicKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A2 (Thu Feb 11 09:49:38 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 79cbf228-16df-4fbl-a385-443546935e74  
 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040  
 00000000000000420092090000000800000004B73C4A24200D0200000040000000100000004200F010000005842  
 005C0500000004000000080000000042007F05000000040000000000000042007C01000000304200940700000024373  
 96362663232382D313664662D346662312D613338352D34343335343639333565373400000000

4

Locate (Private Key)

In: attributes={ objectType='PrivateKey', Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey }}

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type  
Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Private Key)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link  
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:  
Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x0000102 (Public Key Link)  
Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: 79cbf228-16df-4fbl-a385-443546935e74  
 42007801000000F04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040  
 000000000000004200D0200000040000000100000004200F01000000A842005C0500000004000000080000000042  
 00790100000090420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000  
 000400000000420008010000005842000A07000000044C696E6B0000000042000B010000004042004B05000000040000  
 01020000000042004C070000002437396362663232382D313664662D346662312D613338352D343433353436393335653  
 734000000000

Out: uuidPrivateKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A3 (Thu Feb 11 09:49:39 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

	<p><u>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</u></p> <p><u>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66d27b11943</u></p> <p>42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B73C4A342000D0200000040000000100000004200F010000005842005C0500000004000000080000000042007F050000000400000000000000042007C0100000030420094070000002466613036303638632D366662312D343265612D623661322D64363664323762313139343300000000</p>
5	<p><b>Destroy</b></p> <p>In: uuidPrivateKey</p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66d27b11943</u></p> <p>42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B73C4A342000D0200000040000000100000004200F010000005842005C0500000004000000080000000042007F050000000400000000000000042007C0100000030420094070000002466613036303638632D366662312D343265612D623661322D64363664323762313139343300000000</p> <p>Out: uuidPrivateKey</p> <p><u>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A3 (Thu Feb 11 09:49:39 CET 2010)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</u></p> <p><u>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</u></p> <p><u>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66d27b11943</u></p> <p>42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B73C4A342000D0200000040000000100000004200F010000005842005C0500000004000000080000000042007F050000000400000000000000042007C0100000030420094070000002466613036303638632D366662312D343265612D623661322D64363664323762313139343300000000</p>
6	<p><b>Destroy</b></p>

In: uuidPublicKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 79cbf228-16df-4fbl-a385-443546935e74

42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000042000D020000000400000001000000042000F010000004842005C0500000004000000014000000004200790100000030420094070000002437396362663232382D313664662D346662312D613338352D34343335343639333565373400000000

Out: uuidPublicKey

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

42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000004200920900000008000000004B73C4A342000D020000000400000001000000042000F0100000005842005C05000000040000000140000000042007F050000000400000000000000042007C0100000030420094070000002437396362663232382D313664662D346662312D613338352D34343335343639333565373400000000

183  
184

## 99 Key Roll-over

185  
186

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

Formatted: Style Heading 1h1Level 1 Topic  
Heading + Before: 5 pt After: 5..., Outline  
numbered + Level: 1 + Numbering Style: 1, 2,  
3, ... + Start at: 3 + Alignment: Left + Aligned  
at: 0 pt + Indent at: 0 pt

191 **9.19.1 Use-case: Create a Key, Re-key**

192 Create a symmetric key with a specific name, and then use Locate to find the key. After using Re-key to  
 193 create a new key, verify that the name was removed from the existing key and copied to the new key.  
 194 Also verify that the key material for the old key is still retrievable. To clean up, both keys are deleted.  
 195

**Formatted:** Indent: Left: 0 pt, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 36 pt + Indent at: 36 pt, Don't adjust space between Latin and Asian text

**Formatted:** Font: Not Bold

Time	Client A
0	<p>Create (symmetric key)</p> <p>In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='rekeyKey', NameType='00000001' } }</p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</u></p> <p><u>Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey</u></p> <p><u>Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)</u></p> <p><u>42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000011842005C0500000004000000010000000042007901000001004200570500000004000000020000000042009101000000E8420008010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000A070000001443727970746F67726170686963204C656E6774680000000042000B02000000040000000800000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000040000000C00000000420008010000003842000A07000000044E616D650000000042000B0100000020420055070000000872656B65794B657942005405000000040000000100000000</u></p> <p>Out: objectType='00000002', uuidKey</p>

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BA (Thu Feb 11 10:07:06 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B73C8BA42000D0200000004000000010000000042000F010000006842005C050000004000000010000000042007F050000000400000000000000042007C010000004042005705000000400000020000000420094070000002466623536303733352D656636662D343038352D396530612D65623666313339346332313800000000

1

Locate

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

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

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000005842005C05000000400000008000000004200790100000040420008010000003842000A07000000044E616D650000000042000B0100000020420055070000000872656B65794B657942005405000000040000000100000000

Out: uuidKey

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



Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BA (Thu Feb 11 10:07:06 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218  
  
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000004200920900000008000000004B73C8BA42000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F050000000400000000000000042007C0100000030420094070000002466623536303733352D656636662D343038352D396530612D65623666313339346332313800000000

2  
**Rekey**  
In: uuidKey  
  
Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218  
  
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000004000000004200790100000030420094070000002466623536303733352D656636662D343038352D396530612D65623666313339346332313800000000

Out: uuidNewKey  
  
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BB (Thu Feb 11 10:07:07 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: bf6cc1d4-f914-4099-b4d4-453050d8bcf4

	<p><a href="#">42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000042009209000000800000004B73C8BB42000D020000004000000010000000042000F010000005842005C05000000400000004000000042007F05000000400000000000000042007C0100000030420094070000002462663663633164342D663931342D343039392D623464342D34353330353064386263663400000000</a></p>
3	<p><b>Locate</b></p> <p>In: attributes={ Name={ NameValue='rekeyKey', NameType='0000001' } }</p> <p><a href="#">Tag: Request Message (0x420078), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Request Header (0x420077), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</a></p> <p><a href="#">Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</a></p> <p><a href="#">Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</a></p> <p><a href="#">Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)</a></p> <p><a href="#">Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Attribute (0x420008), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name</a></p> <p><a href="#">Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey</a></p> <p><a href="#">Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)</a></p> <p><a href="#">42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042009209000000800000004B73C8BB42000D02000000400000005842005C05000000400000008000000004200790100000040420008010000003842000A07000000044E616D65000000042000B0100000020420055070000000872656B65794B657942005405000000040000000100000000</a></p> <p><b>Out: uuidNewKey</b></p> <p><a href="#">Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</a></p> <p><a href="#">Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</a></p> <p><a href="#">Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B73C8BB (Thu Feb 11 10:07:07 CET 2010)</a></p> <p><a href="#">Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</a></p> <p><a href="#">Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)</a></p> <p><a href="#">Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</a></p> <p><a href="#">Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: bf6ccd4-f914-4099-b4d4-453050d8bcf4</a></p> <p><a href="#">42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000042009209000000800000004B73C8BB42000D020000004000000010000000042000F010000005842005C05000000400000008000000042007F05000000400000000000000042007C0100000030420094070000002462663663633164342D663931342D343039392D623464342D34353330353064386263663400000000</a></p>
4	<p><b>Get Attribute</b></p>

	<p>In: uuidKey, attributeName={Name}</p> <p><b>Out: Operation Failed, Item Not Found</b></p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>  Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)</u></p> <p><u>  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>    Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218</u></p> <p><u>    Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name</u></p> <p>420078010000000A04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D020000000400000001000000004200F010000005842005C05000000040000000B000000004200790100000040420094070000002466623536303733352D656636662D343038352D396530612D6562366631333934633231380000000042000A07000000044E616D6500000000</p> <p><u>Out: uuidKey</u></p> <p><u>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</u></p> <p><u>  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</u></p> <p><u>    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B73C8BB (Thu Feb 11 10:07:07 CET 2010)</u></p> <p><u>    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)</u></p> <p><u>    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</u></p> <p><u>  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</u></p> <p><u>    Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218</u></p> <p>42007B010000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B73C8BB42000D020000000400000001000000004200F010000005842005C05000000040000000B0000000042007F05000000040000000000000042007C0100000030420094070000002466623536303733352D656636662D343038352D396530612D65623666313339346332313800000000</p>
5	<p>Get (symmetric key)</p> <p>In: uuidKey</p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>  Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p>

	<p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218</u></p> <p>42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D020000000400000001000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002466623536303733352D656636662D343038352D396530612D65623666313339346332313800000000</p> <p>Out: objectType = '0000002', uuidKey, symmetricKey</p> <p><u>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BB (Thu Feb 11 10:07:07 CET 2010)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)</u></p> <p><u>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</u></p> <p><u>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218</u></p> <p><u>Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Key Block (0x420040), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001</u></p> <p><u>Tag: Key Value (0x420045), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Key Material (0x420043), Type: Octet String (0x08), Data: BC25617991C49D06536008D076017462</u></p> <p><u>Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)</u></p> <p><u>Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)</u></p> <p>42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B73C8BB42000D0200000004000000010000000042000F01000000C842005C05000000040000000A0000000042007F050000000400000000000000042007C01000000A04200570500000004000000200000000420094070000002466623536303733352D656636662D343038352D396530612D6562366631333934633231380000000042008F010000005842004001000000504200420500000004000000010000000042004501000000184200430800000010BC25617991C49D06536008D0760174624200280500000004000000030000000042002A02000000040000008000000000</p>
6	<p>Destroy</p> <p>In: uuidKey</p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p>

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218  
  
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000004842005C05000000040000001400000000420090100000030420094070000002466623536303733352D656636662D343038352D396530612D65623666313339346332313800000000

Out: uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BC (Thu Feb 11 10:07:08 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218  
  
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000004200920900000008000000004B73C8BC42000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F050000000400000000000000000042007C0100000030420094070000002466623536303733352D656636662D343038352D396530612D65623666313339346332313800000000

7  
Destroy  
In: uuidNewKey  
  
Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: bf6ccid4-f914-4099-b4d4-453050d8bcf4  
  
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000004842005C05000000040000001400000000420090100000030420094070000002462663663633164342D663931342D343039392D623464342D3435333035306438626

	<p><a href="#">366340000000</a></p> <p>Out: uuidNewKey</p> <p><a href="#">Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</a></p> <p><a href="#">Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</a></p> <p><a href="#">Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BC (Thu Feb 11 10:07:08 CET 2010)</a></p> <p><a href="#">Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</a></p> <p><a href="#">Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</a></p> <p><a href="#">Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</a></p> <p><a href="#">Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: bf6ccld4-f914-4099-b4d4-453050d8bcf4</a></p> <p>42007B010000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000004200920900000008000000004B73C8BC42000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002462663663633164342D663931342D343039392D623464342D34353330353064386263663400000000</p>
--	--

196  
197

198 **9.29.2 Use-case: Existing Key Expired, Re-key with Same lifecycle**

199 Create a new symmetric key **with a name**. Then add the *Activation Date* and *Deactivation Date* attributes  
200 based on the timestamp in the response to the Create request. The *Activation Date* is set to a time in the  
201 past and the *Deactivation Date* to a time in the near future. Repeated Get Attribute calls are performed to  
202 verify that the state is first "Active", then subsequently "~~Deactive~~Deactivated". Then issue a Re-key  
203 request, including an *Activation Date* attribute with the value set to the previously specified *Deactivation*  
204 *Date* of the existing key. Verify from the response that the *Activation Date* and *Deactivation Date*  
205 attributes were set correctly (if they are not returned, issue a Get Attribute request). Do a Get Attribute  
206 operation to verify that the state of the new key is "Active". To clean up, both keys are deleted.  
207

**Formatted:** Indent: Left: 0 pt, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 36 pt + Indent at: 36 pt, Don't adjust space between Latin and Asian text

**Formatted:** Font: Not Bold

Time	Client A
0	<p>Create (symmetric key)</p> <p>In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C' }</p> <p><a href="#">Tag: Request Message (0x420078), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Request Header (0x420077), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</a></p> <p><a href="#">Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</a></p> <p><a href="#">Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</a></p> <p><a href="#">Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</a></p>

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm  
Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length  
Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage  
Mask  
Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name  
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:  
Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey  
Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

420078010000001604200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000420000004000000040000000042000F010000011842005C0500000004000000010000000042007901000001004200570500000004000000020000000042009101000000E842008010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000A070000001443727970746F67726170686963204C656E6774680000000042000B0200000004000000080000000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000040000000C00000000420008010000003842000A07000000044E616D65000000042000B0100000020420055070000000872656B65794B65794200540500000004000000100000000

Out: objectType='00000002', uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73FFC7 (Thu Feb 11 14:01:59 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6

42007B010000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000004200920900000008000000004B73FFC742000D0200000004000000010000000042000F0100000006842005C0500000004000000010000000042007F0500000004000000000000000042007C01000000040420057050000000400000020000000420094070000002466626335663365352D343862662D343239342D623735342D30353735613431643933

	623600000000
1	<p>Add Activation Date, Deactivation Date attributes based on Timestamp in previous response (batch)</p> <p>In: uuidKey, attribute={ ActivationDate=' &lt;Timestamp in previous response - 365 days&gt;' }</p> <p>In: uuidKey, attribute={ DeactivationDate=' &lt;Timestamp in previous response + 2 minutes&gt;' }</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)</p> <p>Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BAC4A9CECC650259</p> <p>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6</p> <p>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date</p> <p>Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004992CC47 (Wed Feb 11 14:01:59 CET 2009)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)</p> <p>Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 582C952324F4552F</p> <p>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6</p> <p>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date</p> <p>Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B74003F (Thu Feb 11 14:03:59 CET 2010)</p> <p>42007801000001784200770100000048420069010000002042006A020000000400000001000000042006B02000000040000000000004200100600000080000000000000142000D020000000400000002000000042000F0100000008842005C05000000040000000D000000004200930800000008BAC4A9CECC6502594200790100000060420094070000002466626335663365352D343862662D343239342D623735342D30353735613431643933623600000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B090000000800000004992CC4742000F010000009042005C05000000040000000D0000000042009308000000088582C952324F4552F4200790100000068420094070000002466626335663365352D343862662D343239342D623735342D3035373561343164393362360000000420008010000003042000A0700000011446561637469766174696F6E2044617465000000000000042000B090000000800000004B74003F</p> <p>Out: uuidKey, attribute={ ActivationDate=' &lt;Timestamp in previous response - 1 year&gt;' }</p> <p>Out: uuidKey, attribute={ DeactivationDate=' &lt;Timestamp in previous response + 2 minutes&gt;' }</p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</p> <p>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73FFC7 (Thu Feb 11</p>



14:01:59 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BAC4A9CECC650259

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6

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

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

Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004992CC47 (Wed Feb 11 14:01:59 CET 2009)

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 582C952324F4552F

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6

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

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

Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B74003F (Thu Feb 11 14:03:59 CET 2010)

42007B0100000019842007A01000000048420069010000002042006A0200000004000000010000000042006B02000000040000000000004200920900000008000000004B73FFC742000D02000000400000002000000042000F0100000009842005C050000000400000000D000000004200930800000008BAC4A9CECC65025942007F050000000400000000000000042007C0100000060420094070000002466626335663365352D343862662D343239342D623735342D30353735613431643933623600000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B0900000008000000004992CC474200F01000000A042005C050000000400000000D000000004200930800000008582C952324F4552F42007F050000000400000000000000042007C0100000068420094070000002466626335663365352D343862662D343239342D623735342D3035373561343164393362360000000420008010000002842000A07000000000420008010000003042000A0700000011446561637469766174696F6E204461746500000000000042000B0900000008000000004B74003F

2 Get Attribute \* Repeated until state changes to Deactivated

In: uuidKey, attributeName={'State'}

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)

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

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6

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

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000004200920900000008000000004B73FFC742000D02000000400000002000000042000F0100000009842005C050000000400000000D000000004200930800000008BAC4A9CECC65025942007F050000000400000000000000042007C0100000060420094070000002466626335663365352D343862662D343239342D623735342D30353735613431643933623600000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B0900000008000000004B74003F

[36236000000042000A07000000055374617465000000](#)

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

[Tag: Response Message \(0x42007B\), Type: Structure \(0x01\), Data:](#)

[Tag: Response Header \(0x42007A\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version \(0x420069\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version Major \(0x42006A\), Type: Integer \(0x02\), Data: 0x00000001 \(1\)](#)

[Tag: Protocol Version Minor \(0x42006B\), Type: Integer \(0x02\), Data: 0x00000000 \(0\)](#)

[Tag: Time Stamp \(0x420092\), Type: Date-Time \(0x09\), Data: 0x000000004B73FFC7 \(Thu Feb 11 14:01:59 CET 2010\)](#)

[Tag: Batch Count \(0x42000D\), Type: Integer \(0x02\), Data: 0x00000001 \(1\)](#)

[Tag: Batch Item \(0x42000F\), Type: Structure \(0x01\), Data:](#)

[Tag: Operation \(0x42005C\), Type: Enumeration \(0x05\), Data: 0x0000000B \(Get Attributes\)](#)

[Tag: Result Status \(0x42007F\), Type: Enumeration \(0x05\), Data: 0x00000000 \(Success\)](#)

[Tag: Response Payload \(0x42007C\), Type: Structure \(0x01\), Data:](#)

[Tag: Unique Identifier \(0x420094\), Type: Text String \(0x07\), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6](#)

[Tag: Attribute \(0x420008\), Type: Structure \(0x01\), Data:](#)

[Tag: Attribute Name \(0x42000A\), Type: Text String \(0x07\), Data: State](#)

[Tag: Attribute Value \(0x42000B\), Type: Enumeration \(0x05\), Data: 0x00000002 \(Active\)](#)

[42007B010000000842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000004200920900000008000000004B73FFC742000D0200000004000000010000000042000F0100000008042005C05000000040000000B0000000042007F0500000004000000000000000042007C0100000058420094070000002466626335663365352D343862662D343239342D623735342D3035373561343164393362360000000042000801000000204200A0700000005537461746500000042000B050000004000000020000000](#)

3

Get Attribute

In: uuidKey, attributeName={'State'}

[Tag: Request Message \(0x420078\), Type: Structure \(0x01\), Data:](#)

[Tag: Request Header \(0x420077\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version \(0x420069\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version Major \(0x42006A\), Type: Integer \(0x02\), Data: 0x00000001 \(1\)](#)

[Tag: Protocol Version Minor \(0x42006B\), Type: Integer \(0x02\), Data: 0x00000000 \(0\)](#)

[Tag: Batch Count \(0x42000D\), Type: Integer \(0x02\), Data: 0x00000001 \(1\)](#)

[Tag: Batch Item \(0x42000F\), Type: Structure \(0x01\), Data:](#)

[Tag: Operation \(0x42005C\), Type: Enumeration \(0x05\), Data: 0x0000000B \(Get Attributes\)](#)

[Tag: Request Payload \(0x420079\), Type: Structure \(0x01\), Data:](#)

[Tag: Unique Identifier \(0x420094\), Type: Text String \(0x07\), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6](#)

[Tag: Attribute Name \(0x42000A\), Type: Text String \(0x07\), Data: State](#)

[42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B000000004200790100000040420094070000002466626335663365352D343862662D343239342D623735342D3035373561343164393362360000000042000A07000000055374617465000000](#)

Out: uuidKey, attribute={ State=~~Deactive~~ }~~Deactivated~~ }

	<p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</p> <p>  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</p> <p>    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11 14:04:00 CET 2010)</p> <p>    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>    Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)</p> <p>      Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</p> <p>    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</p> <p>      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6</p> <p>      Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State</p> <p>        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (Deactivated)</p> <p>42007B010000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B74004042000D0200000004000000010000000042000F0100000008042005C05000000040000000B0000000042007F05000000040000000000000042007C0100000058420094070000002466626335663365352D343862662D343239342D623735342D303537356134316439336236000000042008010000002042000A0700000005537461746500000042000B05000000040000000300000000</p>
4	<p><b>Rekey</b></p> <p>In: uuidKey, attribute={ offset='018B8200'FE747E00' (300 days <i>backwards</i>)}</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</p> <p>  Tag: Request Header (0x420077), Type: Structure (0x01), Data:</p> <p>    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>    Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)</p> <p>      Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p>        Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6</p> <p>        Tag: Offset (0x420058), Type: Interval (0x0A), Data: 0xFE747E00</p> <p>420078010000000A04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000005842005C0500000004000000004000000004200790100000040420094070000002466626335663365352D343862662D343239342D623735342D30353735613431643933623600000004200580A00000004FE747E0000000000</p> <p><b>Out: uuidNewKey</b></p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</p> <p>  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</p> <p>    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p>

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11 14:04:00 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92  
  
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B7400404200D02000000400000001000000004200F010000005842005C05000000400000004000000042007F050000004000000000000042007C0100000030420094070000002433383936303262312D636130322D346333632D623561332D63333738396537663263393200000000

5

Get Attribute  
In: uuidNewKey, attributeName={ 'ActivationDate', 'DeactivationDate' }

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date  
  
42007801000000C84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000004200D02000000400000001000000004200F010000008042005C0500000040000000B000000004200790100000068420094070000002433383936303262312D636130322D346333632D623561332D6333373839653766326339320000000042000A07000000F41637469766174696F6E20446174650042000A0700000011446561637469766174696F6E204461746500000000000000

Out: uuidNewKey, attribute={ 'ActivationDate=' <Value of ActivationTime in existing key + 30065 days>', 'DeactivationDate=' <Value of DeactivationDate of existing key + 30065 days>' }

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11 14:04:00 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date  
Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000049E87DC6 (Fri Apr 17 15:01:58 CEST 2009)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date  
Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004BC9B1BE (Sat Apr 17 15:03:58 CEST 2010)  
  
42007B0100000011842007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B74004042000D02000000400000001000000042000F01000000C042005C0500000040000000B0000000042007F0500000040000000000000042007C0100000098420094070000002433383936303262312D636130322D346333632D623561332D63333738396537663263393200000000420008010000002842000A07000000F41637469766174696F6E20446174650042000B0900000008000000049E87DC6420008010000003042000A0700000011446561637469766174696F6E204461746500000000000042000B090000000800000004BC9B1BE

6  
**Get Attribute**  
**In: uuidNewKey, attributeName={'State'}**  
  
Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State  
  
42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000005842005C0500000040000000B000000004200790100000040420094070000002433383936303262312D636130322D346333632D623561332D6333373839653766326339320000000042000A07000000055374617465000000

**Out: uuidNewKey, attribute={ State='Active' }**  
  
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11 14:04:00 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State  
Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active)

42007B010000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000420092090000008000000004B74004042000D020000004000000010000000042000F010000008042005C05000000040000000B0000000042007F05000000040000000000000042007C0100000058420094070000002433383936303262312D636130322D346333632D623561332D6333373839653766326339320000000042008010000002042000A0700000005537461746500000042000B050000004000000020000000

7 Destroy  
In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D020000004000000010000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002466626335663365352D343862662D343239342D623735342D30353735613431643933623600000000

Out: uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B740040 (Thu Feb 11 14:04:00 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6

42007B010000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000420092090000008000000004B74004042000D020000004000000010000000042000F010000005842005C0500000004000000140000000042007F05000000040000000000000042007C01000000304200940700000024666

8	<p><a href="#">26335663365352D343862662D343239342D623735342D30353735613431643933623600000000</a></p> <p><b>Destroy</b>  <b><a href="#">Revoke (symmetric key as cessation of operation) and Destroy</a></b>  <b><a href="#">In (header): batchOrderOption='TRUE'</a></b>  <b><a href="#">In: uuidKey, revocationReasonCode='6'</a></b>  <b>In: uuidNewKey</b></p> <p><a href="#">Tag: Request Message (0x420078), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Request Header (0x420077), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</a>  <a href="#">Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</a>  <a href="#">Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE</a>  <a href="#">Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)</a>  <a href="#">Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)</a>  <a href="#">Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7012417AA1B7394B</a>  <a href="#">Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92</a>  <a href="#">Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000006 (Cessation of Operation)</a>  <a href="#">Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</a>  <a href="#">Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3F8F4F1759704555</a>  <a href="#">Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92</a></p> <p><a href="#">42007801000001284200770100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000042001006000000800000000000000142000D020000000400000002000000042000F010000007042005C0500000004000000130000000042009308000000087012417AA1B7394B4200790100000048420094070000002433383936303262312D636130322D34633632D623561332D63333738396537663263393200000004200810100000010420082050000000400000060000000042000F010000005842005C05000000040000001400000004200930800000083F8F4F17597045554200790100000030420094070000002433383936303262312D636130322D34633632D623561332D63333738396537663263393200000000</a></p> <p><b>Out: uuidNewKey</b>  <b><a href="#">Out: uuidNewKey</a></b></p> <p><a href="#">Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</a>  <a href="#">Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</a>  <a href="#">Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</a>  <a href="#">Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11 14:04:00 CET 2010)</a>  <a href="#">Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)</a>  <a href="#">Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</a></p>
---	---

```

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7012417AA1B7394B
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
  Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3F8F4F1759704555
  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
    Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92

42007B0100000013042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004B7400404200D02000000400000002000000042000F010000006842
005C0500000004000000130000000042009308000000087012417AA1B7394B42007F050000000400000000000000420
07C0100000030420094070000002433383936303262312D636130322D346333632D623561332D63333738396537663263
3932000000042000F010000006842005C0500000004000000140000000042009308000000083F8F4F175970455542007
F05000000040000000000000042007C0100000030420094070000002433383936303262312D636130322D346333632D
623561332D6333373839653766326339320000000

```

208

Formatted: Font: Courier New, 8 pt, Font color: Black

209 **9.39.3 Use-case: Existing Key Compromised, Re-key with same lifecycle**

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

Formatted: Indent: Left: 0 pt, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 36 pt + Indent at: 36 pt, Don't adjust space between Latin and Asian text

215

Formatted: Font: Not Bold

Time	Client A
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='rekeyKey', NameType='00000001' }, ActivationDate='2-<NOW>'}  Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)



Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length  
Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask  
Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date  
Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x00000004B741047 (Thu Feb 11 15:12:23 CET 2010)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name  
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:  
Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey  
Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)  
  
42007801000001904200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000014842005C050000000400000001000000004200790100000130420057050000000400000002000000004200910100000118420008010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000A070000001443727970746F67726170686963204C656E6774680000000042000B02000000040000000800000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000040000000C00000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B0900000008000000004B741047420008010000003842000A07000000044E616D65000000042000B0100000020420055070000000872656B65794B657942005405000000040000000100000000

Out: objectType='00000002', uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B741048 (Thu Feb 11 15:12:24 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781  
  
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000004200920900000008000000004B74104842000D0200000004000000010000000042000F010000006842005C0500000004000000010000000042007F0500000004000000000000000042007C01000000404200570500000004000000200000000420094070000002465656137343262342D393665642D343233382D616664322D35333138396337396637383100000000

1	Get Attribute
---	---------------

	<p>In: uuidKey, attributeName='{State}'</p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u>  <u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u>  <u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u>  <u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u>  <u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u>  <u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u>  <u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u>  <u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)</u>  <u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u>  <u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781</u>  <u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State</u></p> <p>420078010000000A04200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B0000000042007901000000404200940700000002465656137343262342D393665642D343233382D616664322D3533313839633739663738310000000042000A07000000055374617465000000</p> <p>Out: uuidKey, attribute={ State='Active' }</p> <p><u>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</u>  <u>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</u>  <u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u>  <u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u>  <u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u>  <u>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B741048 (Thu Feb 11 15:12:24 CET 2010)</u>  <u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u>  <u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u>  <u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)</u>  <u>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</u>  <u>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</u>  <u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781</u>  <u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u>  <u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State</u>  <u>Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active)</u></p> <p>42007B010000000B842007A01000000048420069010000002042006A0200000004000000010000000042006B02000000040000000000004200920900000008000000004B74104842000D0200000004000000010000000042000F01000000080042005C05000000040000000B0000000042007F050000000400000000000000042007C0100000058420094070000002465656137343262342D393665642D343233382D616664322D35333138396337396637383100000000420008010000002042000A0700000005537461746500000042000B05000000040000000200000000</p>
2	<p>Revoke (symmetric key as compromised)</p> <p>In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceDate='6:'&lt;NOW&gt;'</p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u>  <u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p>

	<p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781</u></p> <p><u>Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000002 (Key Compromise)</u></p> <p><u>Tag: Compromise Occurrence Date (0x420021), Type: Date-Time (0x09), Data: 0x000000004B741048 (Thu Feb 11 15:12:24 CET 2010)</u></p> <p>42007801000000B84200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000007042005C0500000004000000013000000004200790100000058420094070000002465656137343262342D393665642D343233382D616664322D3533313839633739663738310000000420081010000001042008205000000400000002000000004200210900000008000000004B741048</p> <p>Out: uuidKey</p> <p><u>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11 15:12:25 CET 2010)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)</u></p> <p><u>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</u></p> <p><u>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781</u></p> <p>42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000004200920900000008000000004B74104942000D0200000004000000010000000042000F010000005842005C05000000040000000130000000042007F0500000004000000000000000042007C0100000030420094070000002465656137343262342D393665642D343233382D616664322D35333138396337396637383100000000</p>
3	<p>Get Attribute</p> <p>In: uuidKey, attributeName='{State}'</p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p>

	<p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State</u></p> <p>42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B000000004200790100000040420094070000002465656137343262342D393665642D343233382D616664322D3533313839633739663738310000000042000A07000000055374617465000000</p> <p>Out: uuidKey, attribute={ State='Compromised' }</p> <p><u>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11 15:12:25 CET 2010)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)</u></p> <p><u>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</u></p> <p><u>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Compromised)</u></p> <p>42007B010000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74104942000D0200000004000000010000000042000F0100000008042005C05000000040000000B0000000042007F05000000040000000000000042007C0100000058420094070000002465656137343262342D393665642D343233382D616664322D353331383963373966373831000000004200080100000002042000A0700000005537461746500000042000B05000000040000000400000000</p>
4	<p>Rekey</p> <p>In: uuidKey, <del>offset='0'</del></p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781</u></p>

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000040  
0000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000040000000042  
00790100000030420094070000002465656137343262342D393665642D343233382D616664322D3533313839633739663  
7383100000000

Out: uuidNewKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11 15:12:25 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-6ea36a801824

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000040  
000000000000004200920900000008000000004B74104942000D0200000004000000010000000042000F010000005842  
005C0500000004000000040000000042007F05000000040000000000000042007C01000000304200940700000024616  
43363623737342D643030642D343539312D613633342D36656133366138303138323400000000

5

Get Attribute

In: uuidNewKey, attributeName={State}

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)

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

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-6ea36a801824

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

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B0200000040  
0000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B0000000042  
00790100000040420094070000002461643363623737342D643030642D343539312D613633342D3665613336613830313  
83234000000042000A07000000055374617465000000

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

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11 15:12:25 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-6ea36a801824  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State  
Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active)

42007B010000000842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040  
000000000000004200920900000008000000004B74104942000D0200000004000000010000000042000F0100000008042  
005C05000000040000000B0000000042007F05000000040000000000000042007C01000000584200940700000024616  
43363623737342D643030642D343539312D613633342D3665613336613830313832340000000042000801000000204200  
0A07000000005537461746500000042000B05000000040000000200000000

6

**Destroy**  
**In: uuidKey**

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040  
0000000000000042000D0200000004000000010000000042000F0100000004842005C0500000004000000140000000042  
00790100000030420094070000002465656137343262342D393665642D343233382D616664322D3533313839633739663  
7383100000000

**Out: uuidKey**

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11 15:12:25 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

	<p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</u></p> <p><u>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</u></p> <p><u>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781</u></p> <p>42007B010000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000420092090000008000000004B74104942000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F050000000400000000000000042007C0100000030420094070000002465656137343262342D393665642D343233382D616664322D35333138396337396637383100000000</p>
7	<p><u>Revoke (symmetric key as cessation of operation) and Destroy</u></p> <p><u>In (header): batchOrderOption='TRUE'</u></p> <p><u>In: uuidNewKey_revocationReasonCode='6'</u></p> <p><u>In: uuidNewKey</u></p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)</u></p> <p><u>Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7131695CF636735E</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-6ea36a801824</u></p> <p><u>Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000006 (Cessation of Operation)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</u></p> <p><u>Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 1845BCBBF09B5A66</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-6ea36a801824</u></p> <p>42007801000001284200770100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000042001006000000800000000000000142000D0200000004000000020000000042000F010000007042005C0500000004000000130000000042009308000000087131695CF636735E4200790100000048420094070000002461643363623737342D643030642D343539312D613633342D366561333661383031383234000000004200810100000010420082050000000400000006000000042000F010000005842005C0500000004000000140000000042009308000000081845BCBBF09B5A664200790100000030420094070000002461643363623737342D643030642D343539312D613633342D36656133366138303138323400000000</p> <p><u>Out: uuidNewKey</u></p> <p><u>Out: uuidNewKey</u></p> <p><u>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</u></p>

```

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

42007B010000013042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040
0000000000000420092090000008000000004B74104942000D020000000400000002000000042000F010000006842
005C0500000004000000130000000042009308000000087131695CF636735E42007F0500000004000000000000000420
07C0100000030420094070000002461643363623737342D643030642D343539312D613633342D36656133366138303138
3234000000042000F010000006842005C050000000400000014000000042009308000000081845BCBBF09B5A6642007
F0500000004000000000000000042007C0100000030420094070000002461643363623737342D643030642D343539312D
613633342D3665613336613830313832340000000

```

216  
217  
  
218  
219  
220  
221  
222

**9.49.4 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.

Formatted: Font: Courier New, 8 pt, Font color: Black

Formatted: Indent: Left: 0 pt, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 36 pt + Indent at: 36 pt, Don't adjust space between Latin and Asian text

Formatted: Font: Not Bold

Time	Client A
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='rekeyKey', NameType='00000001' }}  Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:





656600000000	
1	<p><b>Locate</b></p> <p>In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } }</p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey</u></p> <p><u>Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)</u></p> <p>42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000005842005C050000000400000008000000004200790100000040420008010000003842000A07000000044E616D65000000042000B0100000020420055070000000872656B65794B657942005405000000040000000100000000</p> <p><b>Out: uuidKey</b></p> <p><u>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742476 (Thu Feb 11 16:38:30 CET 2010)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)</u></p> <p><u>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</u></p> <p><u>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef</u></p> <p>42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000004200920900000008000000004B7424764200D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F05000000040000000000000042007C0100000030420094070000002466303334323539302D663738612D346433342D613266342D34643666633835613536656600000000</p>
2	<p><b>Rekey</b></p> <p>In: uuidKey, attributes={ ActivationDate='000000043B7B630', ProcessStartDate='000000043B7B630', ProtectStopDate='00000005E0C7BB0', DeactivationDate='00000005E0C7BB0' }</p>

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef  
Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date  
Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000043B7B630 (Sun Jan 01 12:00:00 CET 2006)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Process Start Date  
Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000043B7B630 (Sun Jan 01 12:00:00 CET 2006)  
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: 0x00000005E0C7BB0 (Wed Jan 01 12:00:00 CET 2020)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date  
Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x00000005E0C7BB0 (Wed Jan 01 12:00:00 CET 2020)

42007801000001704200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000012842005C050000000400000004000000004200790100000110420094070000002466303334323539302D663738612D346433342D613266342D346436666338356135366566000000042009101000000D8420008010000002842000A070000000F41637469766174696F6E20446174650042000B09000000080000000043B7B630420008010000003042000A070000001250726F63657373205374617274204461746500000000042000B09000000080000000043B7B630420008010000003042000A070000001150726F746563742053746F7020446174650000000000042000B090000000800000005E0C7BB0420008010000003042000A0700000011446561637469766174696F6E20446174650000000000042000B090000000800000005E0C7BB0

Out: uuidNewKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B742477 (Thu Feb 11 16:38:31 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-

	<p><a href="#">ff6ffaa75fbd</a></p> <p><a href="#">42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B74247742000D0200000004000000010000000042000F010000005842005C0500000004000000040000000042007F050000000400000000000000042007C0100000030420094070000002461336661366535632D313339372D346162342D396431322D66663666666161373566626400000000</a></p>
3	<p><b>Get Attribute</b>  <b>In: uuidKey, attributeName={Name}</b>  <b>Out: Operation Failed, Item Not Found</b></p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u>  <u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u>  <u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u>  <u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u>  <u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u>  <u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u>  <u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u>  <u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)</u>  <u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u>  <u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef</u>  <u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name</u></p> <p><a href="#">42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000005842005C050000000400000000B000000004200790100000040420094070000002466303334323539302D663738612D346433342D613266342D346436666338356135366566000000042000A07000000044E616D6500000000</a></p> <p><b>Out: uuidKey</b></p> <p><u>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</u>  <u>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</u>  <u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u>  <u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u>  <u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u>  <u>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742477 (Thu Feb 11 16:38:31 CET 2010)</u>  <u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u>  <u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u>  <u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)</u>  <u>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</u>  <u>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</u>  <u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef</u></p> <p><a href="#">42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B74247742000D0200000004000000010000000042000F010000005842005C050000000400000000B0000000042007F050000000400000000000000042007C0100000030420094070000002466303334323539302D663738612D346433342D613266342D34643666633835613536656600000000</a></p>
4	<p><b>Get Attribute</b>  <b>In: uuidKey, attributeName={ 'ActivationDate', 'ProcessStartDate', 'ProtectStopDate', 'DeactivationDate' }</b></p>

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Process Start Date  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date

42007801000001084200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D020000004000000010000000042000F01000000C042005C050000000400000000B0000000042007901000000A8420094070000002461336661366535632D313339372D346162342D396431322D666636666661613735666264000000042000A07000000F41637469766174696F6E20446174650042000A070000001250726F6365737320537461727420446174650000000000042000A070000001150726F746563742053746F702044617465000000000000042000A0700000011446561637469766174696F6E204461746500000000000000

Out: uuidKey, attribute={ ActivationDate='000000043B7B630', ProcessStartDate='000000043B7B630', ProtectStopDate='00000005E0C7BB0', DeactivationDate='00000005E0C7BB0' }

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B742477 (Thu Feb 11 16:38:31 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date  
Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000043B7B630 (Sun Jan 01 12:00:00 CET 2006)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Process Start Date  
Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000043B7B630 (Sun Jan 01 12:00:00 CET 2006)  
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: 0x00000005E0C7BB0 (Wed

Jan 01 12:00:00 CET 2020)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date  
Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x00000005E0C7BB0 (Wed Jan 01 12:00:00 CET 2020)

42007B0100000018842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000004200920900000008000000004B74247742000D0200000004000000010000000042000F010000013042005C05000000040000000B0000000042007F0500000004000000000000000042007C0100000108420094070000002461336661366535632D313339372D346162342D396431322D66663666666161373566626400000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B09000000080000000043B7B630420008010000003042000A070000001250726F636573732053746172742044617465000000000042000B09000000080000000043B7B630420008010000003042000A070000001150726F746563742053746F70204461746500000000000042000B09000000080000000005E0C7BB0420008010000003042000A0700000011446561637469766174696F6E204461746500000000000042000B090000000800000005E0C7BB0

5  
Locate  
In: attributes={ Name={ NameValue='rekeyKey', NameType='0000001' } }

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

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000F010000005842005C050000000400000008000000004200790100000040420008010000003842000A07000000044E616D650000000042000B0100000020420050570000000872656B65794B657942005405000000040000000100000000

Out: uuidNewKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742477 (Thu Feb 11 16:38:31 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd  
 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74247742000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F05000000040000000000000042007C0100000030420094070000002466336661366535632D313339372D346162342D396431322D66663666666161373566626400000000

**6** **Destroy**  
**In: uuidKey**

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef  
 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000014000000004200790100000030420094070000002466303334323539302D6663738612D346433342D613266342D34643666633835613536656600000000

**Out: uuidKey**

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742478 (Thu Feb 11 16:38:32 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef  
 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74247842000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F05000000040000000000000042007C0100000030420094070000002466303334323539302D6663738612D346433342D613266342D34643666633835613536656600000000

**7** **Revoke (symmetric key as cessation of operation) and Destroy**  
**In (header): batchOrderOption='TRUE'**

[In: uuidNewKey\\_revocationReasonCode='6'](#)

[In: uuidNewKey](#)

[Tag: Request Message \(0x420078\), Type: Structure \(0x01\), Data:](#)

[Tag: Request Header \(0x420077\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version \(0x420069\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version Major \(0x42006A\), Type: Integer \(0x02\), Data: 0x00000001 \(1\)](#)

[Tag: Protocol Version Minor \(0x42006B\), Type: Integer \(0x02\), Data: 0x00000000 \(0\)](#)

[Tag: Batch Order Option \(0x420010\), Type: Boolean \(0x06\), Data: TRUE](#)

[Tag: Batch Count \(0x42000D\), Type: Integer \(0x02\), Data: 0x00000002 \(2\)](#)

[Tag: Batch Item \(0x42000F\), Type: Structure \(0x01\), Data:](#)

[Tag: Operation \(0x42005C\), Type: Enumeration \(0x05\), Data: 0x00000013 \(Revoke\)](#)

[Tag: Unique Batch Item ID \(0x420093\), Type: Octet String \(0x08\), Data: 3DC816BB39869D07](#)

[Tag: Request Payload \(0x420079\), Type: Structure \(0x01\), Data:](#)

[Tag: Unique Identifier \(0x420094\), Type: Text String \(0x07\), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd](#)

[Tag: Revocation Reason \(0x420081\), Type: Structure \(0x01\), Data:](#)

[Tag: Revocation Reason Code \(0x420082\), Type: Enumeration \(0x05\), Data: 0x00000006 \(Cessation of Operation\)](#)

[Tag: Batch Item \(0x42000F\), Type: Structure \(0x01\), Data:](#)

[Tag: Operation \(0x42005C\), Type: Enumeration \(0x05\), Data: 0x00000014 \(Destroy\)](#)

[Tag: Unique Batch Item ID \(0x420093\), Type: Octet String \(0x08\), Data: 32B517312FD5B558](#)

[Tag: Request Payload \(0x420079\), Type: Structure \(0x01\), Data:](#)

[Tag: Unique Identifier \(0x420094\), Type: Text String \(0x07\), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd](#)

42007801000001284200770100000048420069010000002042006A02000000400000001000000042006B0200000040  
000000000000042001006000000800000000000000142000D02000000400000002000000042000F010000007042  
005C05000000400000013000000004200930800000083DC816BB39869D0742007901000000484200940700000024613  
36661366535632D313339372D346162342D396431322D666636666661613735666264000000042008101000000104200  
820500000040000006000000042000F010000005842005C05000000400000014000000042009308000000832B51  
7312FD5B5584200790100000030420094070000002461336661366535632D313339372D346162342D396431322D666636  
66666161373566626400000000

[Out: uuidNewKey](#)

[Out: uuidNewKey](#)

[Tag: Response Message \(0x42007B\), Type: Structure \(0x01\), Data:](#)

[Tag: Response Header \(0x42007A\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version \(0x420069\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version Major \(0x42006A\), Type: Integer \(0x02\), Data: 0x00000001 \(1\)](#)

[Tag: Protocol Version Minor \(0x42006B\), Type: Integer \(0x02\), Data: 0x00000000 \(0\)](#)

[Tag: Time Stamp \(0x420092\), Type: Date-Time \(0x09\), Data: 0x00000004B742478 \(Thu Feb 11 16:38:32 CET 2010\)](#)

[Tag: Batch Count \(0x42000D\), Type: Integer \(0x02\), Data: 0x00000002 \(2\)](#)

[Tag: Batch Item \(0x42000F\), Type: Structure \(0x01\), Data:](#)

[Tag: Operation \(0x42005C\), Type: Enumeration \(0x05\), Data: 0x00000013 \(Revoke\)](#)

[Tag: Unique Batch Item ID \(0x420093\), Type: Octet String \(0x08\), Data: 3DC816BB39869D07](#)

[Tag: Result Status \(0x42007F\), Type: Enumeration \(0x05\), Data: 0x00000000 \(Success\)](#)

[Tag: Response Payload \(0x42007C\), Type: Structure \(0x01\), Data:](#)

[Tag: Unique Identifier \(0x420094\), Type: Text String \(0x07\), Data: a3fa6e5c-1397-4ab4-9d12-](#)



```

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

42007B010000013042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000420092090000008000000004B7424784200D0200000004000000020000000042000F010000006842
005C0500000004000000130000000042009308000000083DC816BB39869D0742007F0500000004000000000000000420
07C0100000030420094070000002461336661366535632D313339372D346162342D396431322D66663666666161373566
62640000000042000F010000006842005C05000000040000001400000000420093080000000832B517312FD5B55842007
F050000000400000000000000042007C0100000030420094070000002461336661366535632D313339372D346162342D
396431322D666636666661613735662640000000

```

Formatted: Font: Courier New, 8 pt

223  
224  
  
225  
226  
227  
228  
229

**9.59.5 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.

Formatted: Indent: Left: 0 pt, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 36 pt + Indent at: 36 pt, Don't adjust space between Latin and Asian text

Formatted: Font: Not Bold

Time	Client-A	Client-B
0	<p><u>Client A:</u> Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue=' rekeyKey', NameType='00000001' }, ActivationDate='2'&lt;NOW&gt; }</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</p>	

Formatted Table

<p>Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:</p> <p>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm</p> <p>Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)</p> <p>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length</p> <p>Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)</p> <p>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask</p> <p>Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)</p> <p>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name</p> <p>Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:</p> <p>Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey</p> <p>Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)</p> <p>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date</p> <p>Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x00000004B74262C (Thu Feb 11 16:45:48 CET 2010)</p> <p>42007801000001904200770100000038420069010000002042006A020000000400000010000000042006B020000000400000000000000042000D020000000400000010000000042000F010000014842005C050000004000000100000000420079010000013042005705000000040000000200000004200910100000118420008010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000420008010000003042000A070000001443727970746F67726170686963204C656E677468000000042000B020000004000000800000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000000000420008010000003842000A07000000044E616D65000000042000B010000020420055070000000872656B65794B65794200540500000004000000010000000420008010000002842000A07000000F41637469766174696F6E20446174650042000B090000000800000004B74262C</p> <p>Out: objectType='00000002', uuidKey</p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</p> <p>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data:</p>	
---	--

	<p>0x00000004B74262D (Thu Feb 11 16:45:49 CET 2010)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)</p> <p>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</p> <p>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</p> <p>Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce</p> <p>42007B01000000C042007A0100000048420069010000002042006A02000000040000010000000042006B02000000040000000000000042009209000000800000004B74262D42000D0200000004000000010000000042000F010000006842005C050000004000000010000000042007F05000000040000000000000000000042007C010000004042005705000000040000000200000000420094070000002463613336386533332D646333642D346337632D386636642D32363238393562633331636500000000</p>	
1	<p><b>Client A:</b></p> <p>Get (symmetric key)</p> <p>In: uuidKey</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)</p> <p>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce</p> <p>42007801000000904200770100000038420069010000002042006A02000000040000010000000042006B02000000040000000000000042000D02000000040000010000000042000F010000004842005C05000000040000000A0000000004200790100000030420094070000002463613336386533332D646333642D346337632D386636642D32363238393562633331636500000000</p> <p>Out: objectType = '00000002', uuidKey, symmetricKey</p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</p> <p>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p>	

	<p>Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262D (Thu Feb 11 16:45:49 CET 2010)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)</p> <p>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</p> <p>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</p> <p>Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce</p> <p>Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:</p> <p>Tag: Key Block (0x420040), Type: Structure (0x01), Data:</p> <p>Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001</p> <p>Tag: Key Value (0x420045), Type: Structure (0x01), Data:</p> <p>Tag: Key Material (0x420043), Type: Octet String (0x08), Data: F43C7798AACB22B1411A8773C199708B</p> <p>Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)</p> <p>Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)</p> <p>42007B010000012042007A0100000048420069010000002042006A0200000000400000010000000042006B02000000040000000000000000420092090000000800000004B74262D42000D0200000004000000010000000042000F01000000C842005C05000000040000000A00000000042007F0500000004000000000000000000042007C01000000A042005705000000040000000200000000420094070000002463613336386533332D646333642D346337632D386636642D323632383935626333316365000000042008F01000000584200400100000050420042050000000400000001000000042004501000000184200430800000010F43C7798AACB22B1411A8773C199708B4200280500000004000000030000000042002A02000000040000000800000000</p>	
2	<p><b>Client A:</b></p> <p>Obtain Lease</p> <p>In: uuidKey</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data:</p>	

	<p>0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)</p> <p>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce</p> <p>42007801000000904200770100000038420069010000002042006A020000000400000010000000042006B020000000400000000000000042000D020000000400000010000000042000F010000004842005C050000000400000010000000004200790100000030420094070000002463613336386533332D646333642D346337632D386636642D32363238393562633331636500000000</p> <p>Out: uuidKey, leaseTime, lastChangeDate</p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</p> <p>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262E (Thu Feb 11 16:45:50 CET 2010)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)</p> <p>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</p> <p>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce</p> <p>Tag: Lease Time (0x420049), Type: Interval (0x0A), Data: 0x00000010</p> <p>Tag: Last Change Date (0x420048), Type: Date-Time (0x09), Data: 0x000000004B74262D (Thu Feb 11 16:45:49 CET 2010)</p> <p>42007B01000000D042007A0100000048420069010000002042006A020000000400000010000000042006B0200000004000000000000000420092090000000800000004B74262E42000D0200000004000000010000000042000F010000007842005C050000000400000010000000042007F0500000004000000000000000000042007C01000000050420094070000002463613336386533332D646333642D346337632D386636642D323632383935626333316365000000004200490A000000040000001000000004200480900000008000000004B74262D</p>	
3	<p>Client B:</p> <p>Revoke (symmetric key as compromised)</p> <p>In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceDate='&lt;NOW&gt;'</p>	<p>Revoke (symmetric key as compromised)</p> <p>In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceDate='6'</p>

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
   Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
     Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
       Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
       Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
       Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
       Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
         Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)  
         Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
           Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce  
           Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:  
             Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000002 (Key Compromise)  
             Tag: Compromise Occurrence Date (0x420021), Type: Date-Time (0x09), Data: 0x00000004B74262E (Thu Feb 11 16:45:50 CET 2010)

Out: uuidKey

42007801000000B84200770100000038420069010000002042006A020000000040  
 00000010000000042006B0200000004000000000000000042000D020000000400  
 0000010000000042000F010000007042005C050000000400000013000000000420  
 0790100000058420094070000002463613336386533332D646333642D34633763  
 2D386636642D32363238393562633331636500000000420081010000001042008  
 2050000000400000002000000004200210900000008000000004B74262E

Out: uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
   Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
     Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
       Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
       Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
       Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B74262E (Thu Feb 11 16:45:50 CET 2010)  
       Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
       Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
         Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)  
         Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
         Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
           Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce

42007B01000000B042007A0100000048420069010000002042006A020000000040  
 00000010000000042006B02000000040000000000000000420092090000000800

	<p>0000004B74262E42000D0200000004000000010000000042000F0100000058420  05C0500000004000000130000000042007F050000000400000000000000004200  7C01000000030420094070000002463613336386533332D646333642D346337632  D386636642D32363238393562633331636500000000</p>	
4	<p><b>Client B:</b>  <b>Rekey</b>  <b>In: uuidKey</b></p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:  Tag: Request Header (0x420077), Type: Structure (0x01), Data:  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce</p> <p>42007801000000904200770100000038420069010000002042006A020000000040  00000010000000042006B0200000004000000000000000042000D020000000400  0000100000000042000F010000004842005C05000000040000000400000000420  0790100000030420094070000002463613336386533332D646333642D34633763  2D386636642D32363238393562633331636500000000</p> <p><b>Out: uuidNewKey</b></p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f</p>	<p><b>Rekey</b>  <b>In: uuidKey, offset='0'</b>  <b>Out: uuidNewKey</b></p>

	<pre>42007B01000000B042007A0100000048420069010000002042006A02000000040 0000010000000042006B02000000040000000000000000420092090000000800 0000004B74262F42000D0200000004000000010000000042000F0100000058420 05C0500000004000000040000000042007F050000000400000000000000004200 7C0100000030420094070000002435396662663831642D353734662D346634662 D393538312D37373835646335393366356600000000</pre>	
5	<p><u>Client A:</u> Obtain Lease In: uuidKey</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:  Tag: Request Header (0x420077), Type: Structure (0x01), Data:  Tag: Protocol Version (0x420069), Type: Structure (0x01),  Data:  Tag: Protocol Version Major (0x42006A), Type: Integer  (0x02), Data: 0x00000001 (1)  Tag: Protocol Version Minor (0x42006B), Type: Integer  (0x02), Data: 0x00000000 (0)  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data:  0x00000001 (1)  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data:  0x00000010 (Obtain Lease)  Tag: Request Payload (0x420079), Type: Structure (0x01),  Data:  Tag: Unique Identifier (0x420094), Type: Text String  (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc3lce</p> <pre>42007801000000904200770100000038420069010000002042006A02000000040 0000010000000042006B0200000004000000000000000042000D020000000400 000010000000042000F010000004842005C05000000040000001000000000420 0790100000030420094070000002463613336386533332D646333642D34633763 2D386636642D32363238393562633331636500000000</pre> <p>Out: Operation Failed, Permission Denied</p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  Tag: Protocol Version (0x420069), Type: Structure (0x01),  Data:  Tag: Protocol Version Major (0x42006A), Type: Integer  (0x02), Data: 0x00000001 (1)  Tag: Protocol Version Minor (0x42006B), Type: Integer  (0x02), Data: 0x00000000 (0)  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data:  0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data:  0x00000001 (1)  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data:  0x00000010 (Obtain Lease)  Tag: Result Status (0x42007F), Type: Enumeration (0x05),  Data: 0x00000001 (Operation Failed)  Tag: Result Reason (0x42007E), Type: Enumeration (0x05),</p>	



	<p>Data: 0x0000000C (Permission Denied)</p> <p>Tag: Result Message (0x42007D), Type: Text String (0x07), Data: CO is in state Compromised, no lease given</p> <p>42007B010000000C042007A0100000048420069010000002042006A02000000040 00000010000000042006B02000000040000000000000000420092090000000800 0000004B74262F42000D020000000400000001000000004200F0100000068420 05C0500000004000000100000000042007F050000000400000001000000004200 7E05000000040000000C0000000042007D070000002A434F20697320696E20737 461746520436F6D70726F6D697365642C206E6F206C6561736520676976656E00 0000000000</p>	
6	<p><u>Client A:</u></p> <p>Locate (symmetric key)</p> <p>In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' }}</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)</p> <p>42007801000000A04200770100000038420069010000002042006A020000000040 00000010000000042006B0200000004000000000000000042000D020000000400 0000010000000042000F010000005842005C05000000040000000800000000420 0790100000040420008010000003842000A07000000044E616D65000000004200 0B0100000020420055070000000872656B65794B6579420054050000000400000 001000000000</p> <p>Out: uuidNewKey</p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer</p>	

	<pre> (0x02), Data: 0x00000001 (1)   Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)   Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)   Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)   Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:   Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)   Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)   Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:   Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f  42007B01000000B042007A0100000048420069010000002042006A020000000040 0000010000000042006B02000000040000000000000000420092090000000800 000004B74262F42000D0200000004000000010000000042000F0100000058420 05C0500000004000000080000000042007F0500000004000000000000004200 7C0100000030420094070000002435396662663831642D353734662D346634662 D393538312D37373835646335393366356600000000 </pre>	
7	<p><b>Client A:</b>  Get (symmetric key)  In: uuidNewKey</p> <pre> Tag: Request Message (0x420078), Type: Structure (0x01), Data:   Tag: Request Header (0x420077), Type: Structure (0x01), Data:     Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:       Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)       Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)       Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)       Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:       Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)       Tag: Request Payload (0x420079), Type: Structure (0x01), Data:       Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f  42007801000000904200770100000038420069010000002042006A020000000040 0000010000000042006B0200000004000000000000000042000D020000000400 000010000000042000F010000004842005C05000000040000000A00000000420 0790100000030420094070000002435396662663831642D353734662D34663466 2D393538312D37373835646335393366356600000000 </pre> <p>Out: objectType = '00000002', uuidNewKey, newSymmetricKey</p> <pre> Tag: Response Message (0x42007B), Type: Structure (0x01), Data:   Tag: Response Header (0x42007A), Type: Structure (0x01), Data: </pre>	

	<p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B74262F (Thu Feb 11 16:45:51 CET 2010)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)</p> <p>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</p> <p>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</p> <p>Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f</p> <p>Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:</p> <p>Tag: Key Block (0x420040), Type: Structure (0x01), Data:</p> <p>Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001</p> <p>Tag: Key Value (0x420045), Type: Structure (0x01), Data:</p> <p>Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 173E9499F7C573712AFB9883B5DF2BCE</p> <p>Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)</p> <p>Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)</p> <p>42007B0100000012042007A0100000048420069010000002042006A020000000040000010000000042006B0200000004000000000000000420092090000000800000004B74262F42000D020000000400000001000000042000F01000000C842005C05000000040000000A0000000042007F05000000040000000000000000042007C01000000A04200570500000004000000020000000420094070000002435396662663831642D353734662D346634662D393538312D373738356463353933663566000000042008F0100000058420040010000005042004205000000040000001000000042004501000000184200430800000010173E9499F7C573712AFB9883B5DF2BCE4200280500000004000000030000000042002A02000000040000000800000000</p>	
8	<p><b>Client A:</b> Obtain Lease In: uuidNewKey</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p>	

	<p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)</p> <p>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f</p> <p>42007801000000904200770100000038420069010000002042006A0200000000400000010000000042006B02000000400000000000000042000D02000000040000010000000042000F010000004842005C050000000400000010000000004200790100000030420094070000002435396662663831642D353734662D346634662D393538312D37373835646335393366356600000000</p> <p>Out: uuidNewKey, leaseTime, lastChangeDate</p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</p> <p>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)</p> <p>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</p> <p>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f</p> <p>Tag: Lease Time (0x420049), Type: Interval (0x0A), Data: 0x00000000</p> <p>Tag: Last Change Date (0x420048), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)</p> <p>42007B01000000D042007A0100000048420069010000002042006A0200000000400000010000000042006B020000004000000000000000420092090000000800000004B74262F42000D020000004000000010000000042000F0100000007842005C0500000004000000100000000042007F05000000040000000000000000000042007C01000000050420094070000002435396662663831642D353734662D346634662D393538312D373738356463353933663566000000004200490A00000004000000000000004200480900000008000000004B74262F</p>	
9	<p><u>Client A:</u> Destroy In: uuidKey</p>	

	<p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</p> <p>  Tag: Request Header (0x420077), Type: Structure (0x01), Data:</p> <p>    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>      Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>      Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>        Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</p> <p>        Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p>          Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce</p> <p>42007801000000904200770100000038420069010000002042006A0200000000400000010000000042006B020000000400000000000000042000D02000000040000010000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002463613336386533332D64633642D346337632D386636642D32363238393562633331636500000000</p> <p>Out: uuidKey</p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</p> <p>  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</p> <p>    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>      Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)</p> <p>      Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>      Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>        Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</p> <p>        Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</p> <p>        Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</p> <p>          Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce</p> <p>42007B01000000B042007A0100000048420069010000002042006A02000000004000000100000000420092090000000800000004B74262F42000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F050000000400000000000000000042007C0100000030420094070000002463613336386533332D64633642D346337632D386636642D32363238393562633331636500000000</p>	
10	<p><a href="#">Client A:</a>  <a href="#">Revoke (symmetric key as cessation of operation) and Destroy</a></p>	

In (header): batchOrderOption='TRUE'  
In: uuidNewKey, revocationReasonCode='6'  
In: uuidNewKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)  
Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3748B9E243205BA7  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f  
Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:  
Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000006 (Cessation of Operation)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 04EAF416D0BEB50D  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f

42007801000001284200770100000048420069010000002042006A020000000040  
0000010000000042006B0200000004000000000000000420010060000000800  
000000000000142000D020000000400000002000000042000F0100000070420  
05C0500000004000000130000000042009308000000083748B9E243205BA74200  
790100000048420094070000002435396662663831642D353734662D346634662  
D393538312D37373835646335393366356600000004200810100000010420082  
05000000400000006000000042000F010000005842005C0500000040000001  
40000000420093080000000804EAF416D0BEB50D420079010000003042009407  
0000002435396662663831642D353734662D346634662D393538312D373738356  
46335393366356600000000

Out: uuidNewKey  
Out: uuidNewKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

<pre> Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3748B9E243205BA7 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 04EAF416D0BEB50D Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f  42007B0100000013042007A01000000048420069010000002042006A020000000040 0000010000000042006B02000000040000000000000000420092090000000800 0000004B74262F42000D020000000400000002000000042000F0100000068420 05C0500000004000000130000000042009308000000083748B9E243205BA74200 7F050000000400000000000000042007C0100000030420094070000002435396 662663831642D353734662D346634662D393538312D37373738356463353936635 660000000042000F010000006842005C050000000400000014000000004200930 8000000804EAF416D0BEB50D42007F05000000040000000000000042007C01 00000030420094070000002435396662663831642D353734662D346634662D393 538312D3737383564633539366356600000000 </pre>	
---	--

Formatted: Font: Courier New, 8 pt

230

231 **1010 Archival**

Formatted: Style Heading 1h1Level 1 Topic Heading + Before: 5 pt After: 5..., Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 3 + Alignment: Left + Aligned at: 0 pt + Indent at: 0 pt

232

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

236 **10.110.1 Use-case: Create a Key, Archive and Recover it**

Formatted: Font: Not Bold

237 Create a symmetric key with a specified name, then use Locate to find the key and get the key. Archive  
238 the key (asynchronous operation, use Poll until it completes) and use Get and Locate on it, but both fail.  
239 Add the Storage Status Mask to the Locate-command, indicating to the server to search in both online

Formatted: Indent: Left: 0 pt, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 36 pt + Indent at: 36 pt, Don't adjust space between Latin and Asian text

240 and archived storage. The Locate finds the key. Recover the key from the archive (also asynchronous),  
 241 both Locate and Get succeed.  
 242

Time	Client A
0	<p>Create (symmetric key)</p> <p>In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='archiveKey', NameType='00000001' }}</p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</u></p> <p><u>Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Name Value (0x420055), Type: Text String (0x07), Data: archiveKey</u></p> <p><u>Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)</u></p> <p>42007801000001684200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000012042005C050000000400000001000000004200790100000108420057050000000400000002000000042009101000000F042008010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000A070000001443727970746F67726170686963204C656E677468000000042000B02000000040000000800000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000040000000C000000004200080100000004042000A07000000044E616D65000000042000B0100000028420055070000000A617263686976654B65790000000000042005405000000040000000100000000</p> <p>Out: objectType='00000002', uuidKey</p> <p><u>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</u></p>



	<p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FA3 (Fri Feb 12 10:30:11 CET 2010)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)</p> <p>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</p> <p>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</p> <p>Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f</p> <p>42007B0100000000042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B751FA34200D020000004000000010000000042000F010000006842005C0500000004000000010000000042007F0500000004000000000000000000042007C01000000404200570500000004000000200000004200940700000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000</p>
1	<p>Locate</p> <p>In: attributes={ Name={ NameValue='archiveKey', NameType='00000001' } }</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)</p> <p>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type</p> <p>Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</p> <p>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name</p> <p>Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:</p> <p>Tag: Name Value (0x420055), Type: Text String (0x07), Data: archiveKey</p> <p>Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)</p> <p>4200780100000000B84200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B751FA34200D020000004000000010000000042000F010000006842005C0500000004000000010000000042007F0500000004000000000000000000042007C01000000404200570500000004000000200000004200940700000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000</p> <p>Out: uuidKey</p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</p>

	<p>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FA6 (Fri Feb 12 10:30:14 CET 2010)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)</p> <p>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</p> <p>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f</p> <p>42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B751FA642000D02000000400000001000000042000F010000005842005C050000000400000008000000042007F0500000004000000000000042007C0100000030420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000</p>
2	<p>Get (symmetric key) In: uuidKey</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)</p> <p>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f</p> <p>42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000420092090000004000000004000000010000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000</p> <p>Out: objectType = '00000002', uuidKey, symmetricKey</p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</p> <p>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FA7 (Fri Feb 12 10:30:15 CET 2010)</p> <p>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)</p> <p>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</p>

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f  
Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:  
Tag: Key Block (0x420040), Type: Structure (0x01), Data:  
Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001  
Tag: Key Value (0x420045), Type: Structure (0x01), Data:  
Tag: Key Material (0x420043), Type: Octet String (0x08), Data: C3200B1291BA648DB9089DED3073DE74  
Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)  
Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)  
  
42007B0100000012042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000420092090000008000000004B751FA74200D020000004000000010000000042000F01000000C842005C0500000040000000A000000042007F0500000004000000000000042007C01000000A04200570500000040000000000000420094070000002430643535323136302D666230342D346637632D386137332D666566393035623231633066000000042008F010000005842004001000000504200420500000004000000010000000042004501000000184200430800000010C3200B1291BA648DB9089DED3073DE744200280500000004000000030000000042002A02000000040000008000000000

3

Archive

In: uuidKey, asynchronousIndicator='true'

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000015 (Archive)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f  
  
42007801000000A04200770100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000F01000000C842005C0500000040000001500000004200790100000030420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000

Out: asynchronousCorrelationValue

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FA7 (Fri Feb 12 10:30:15 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000015 (Archive)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Operation Pending)  
Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:  
F17893DB51652969  
  
42007B010000008842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040  
000000000000004200920900000008000000004B751FA742000D0200000004000000010000000042000F010000003042  
005C0500000004000000150000000042007F05000000040000000200000000420006080000008F17893DB51652969

4

**Poll\***

**In: asynchronousCorrelationValue**

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:  
F17893DB51652969  
  
42007801000000704200770100000038420069010000002042006A0200000004000000010000000042006B02000000040  
0000000000000042000D0200000004000000010000000042000F010000002842005C05000000040000001A0000000042  
00790100000010420006080000008F17893DB51652969

**Out: uuidKey**

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAA (Fri Feb 12  
10:30:18 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000015 (Archive)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-  
fef905b21c0f  
  
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040  
000000000000004200920900000008000000004B751FAA42000D0200000004000000010000000042000F010000005842  
005C0500000004000000150000000042007F05000000040000000000000042007C01000000304200940700000024306  
43535323136302D666230342D346637632D386137332D66656639303562323163306600000000

5

**Get (symmetric key)**

In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000

Out: Operation Failed, ~~Item Not Found~~Object Archived

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAC (Fri Feb 12 10:30:20 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)  
Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x0000000D (Object Archived)  
Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Object is archived

42007B01000000A842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000004200920900000008000000004B751FAC4200D020000004000000010000000042000F010000005042005C05000000040000000A0000000042007F0500000004000000010000000042007E05000000040000000D0000000042007D07000000124F626A656374206973206172636869766564000000000000

6

Get Attribute (Archive Date)

In: uuidKey, attributeName='ArchiveDate'

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)

	<p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u>  <u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f</u>  <u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Archive Date</u></p> <p>42007801000000A84200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000420000B0200000004000000000000420000D020000000400000000100000000420000F010000006042005C050000000400000000B000000004200790100000048420094070000002430643535323136302D666230342D346637632D386137332D666566393035623231633066000000042000A070000000C41726368697665204461746500000000</p> <p><u>Out: uuidKey, attribute={ ArchiveDate }</u></p> <p><u>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</u>  <u>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</u>  <u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u>  <u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u>  <u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u>  <u>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B751FAC (Fri Feb 12 10:30:20 CET 2010)</u>  <u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u>  <u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u>  <u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)</u>  <u>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</u>  <u>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</u>  <u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f</u>  <u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u>  <u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Archive Date</u>  <u>Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x00000004B751FAA (Fri Feb 12 10:30:18 CET 2010)</u></p> <p>42007B01000000E042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000420000B0200000004000000000000420000D020000000400000000100000000420000F010000008842005C050000000400000000B0000000042007F050000000400000000000000042007C0100000060420094070000002430643535323136302D666230342D346637632D386137332D6665663930356232316330660000000420008010000002842000A070000000C417263686976652044617465000000042000B090000000800000004B751FAA</p>
67	<p>Locate</p> <p>In: attributes={ Name={ NameValue='archiveKey', NameType='00000001' } }</p> <p><u>Out: Operation Failed, Item Not Found</u></p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u>  <u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u>  <u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u>  <u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u>  <u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u>  <u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u>  <u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u>  <u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)</u>  <u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u>  <u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u>  <u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type</u>  <u>Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric</u></p>

	<p><u>Key)</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Name Value (0x420055), Type: Text String (0x07), Data: archiveKey</u></p> <p><u>Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)</u></p> <p><u>420078010000000D84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D020000000400000001000000004200F010000009042005C050000000400000008000000004200790100000078420008010000002842000A070000000B4F626A6563742054797065000000000042000B05000000040000200000000420008010000004042000A07000000044E616D65000000042000B0100000028420055070000000A617263686976654B65790000000000042005405000000040000000100000000</u></p> <p><u>Out: &lt;empty response payload&gt;</u></p> <p><u>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Response Header (0x42007A), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAC (Fri Feb 12 10:30:20 CET 2010)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)</u></p> <p><u>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</u></p> <p><u>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: null</u></p> <p><u>42007B0100000008042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B751FAC42000D020000000400000001000000004200F010000002842005C0500000004000000080000000042007F0500000004000000000000000042007C0100000000</u></p>
78	<p>Locate</p> <p>In: storageStatusMask='00000003', attributes={ Name={ NameValue='archiveKey', NameType='00000001' } }</p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Storage Status Mask (0x42008E), Type: Integer (0x02), Data: 0x00000003 (3)</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type</u></p> <p><u>Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</u></p> <p><u>Tag: Attribute (0x420008), Type: Structure (0x01), Data:</u></p>

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

42007801000000E84200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F01000000A042005C050000000400000008000000000420079010000008842008E02000000040000000300000000420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000020000000420008010000004042000A07000000044E616D65000000042000B0100000028420055070000000A617263686976654B65790000000000042005405000000040000000100000000

Out: uuidKey

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B751FAC4200D02000000400000010000000042000F010000005842005C0500000004000000080000000042007F050000000400000000000000042007C0100000030420094070000002430643535323136302D666230342D346637632D386137332D6665663930356232316330600000000

89

Recover  
In: uuidKey, asynchronousIndicator='true'

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

42007801000000A04200770100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200070600000080000000000000014200D0200000004000000010000000042000F010000004842005C0500000004000000016000000004200790100000030420094070000002430643535323136302D666230342D3466376



32D386137332D66656639303562323163306600000000

Out: asynchronousCorrelationValue

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAC (Fri Feb 12 10:30:20 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000016 (Recover)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Operation Pending)

Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: DDBB075607727F3F

42007B010000008842007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B751FAC42000D0200000004000000010000000042000F010000003042005C0500000004000000160000000042007F050000000400000002000000004200060800000008DDBB075607727F3F

910

Poll\*

In: asynchronousCorrelationValue

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll)

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

Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: DDBB075607727F3F

42007801000000704200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000002842005C050000000400000001A0000000042007901000000104200060800000008DDBB075607727F3F

Out: uuidKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FB3 (Fri Feb 12 10:30:27 CET 2010)

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

Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000016 (Recover)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f  
  
42007B010000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B751FB342000D0200000004000000010000000042000F010000005842005C050000004000000160000000042007F05000000040000000000000042007C0100000030420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000

4011 Get (symmetric key)  
In: uuidKey  
  
Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f  
  
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000420092090000000400000000400000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000  
  
Out: objectType = '00000002', uuidKey, symmetricKey  
  
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FB3 (Fri Feb 12 10:30:27 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f  
Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:  
Tag: Key Block (0x420040), Type: Structure (0x01), Data:  
Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001

Tag: Key Value (0x420045), Type: Structure (0x01), Data:  
Tag: Key Material (0x420043), Type: Octet String (0x08), Data:  
 C3200B1291BA648DB9089DED3073DE74  
Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)  
Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)  
  
 42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040  
 0000000000000420092090000008000000004B751FB34200D0200000040000000100000004200F01000000C842  
 005C05000000040000000A0000000042007F05000000040000000000000042007C01000000A04200570500000004000  
 000200000000420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163  
 3066000000042008F010000005842004001000000504200420500000040000000100000000420045010000001842004  
 30800000010C3200B1291BA648DB9089DED3073DE744200280500000004000000030000000042002A020000004000000  
 8000000000

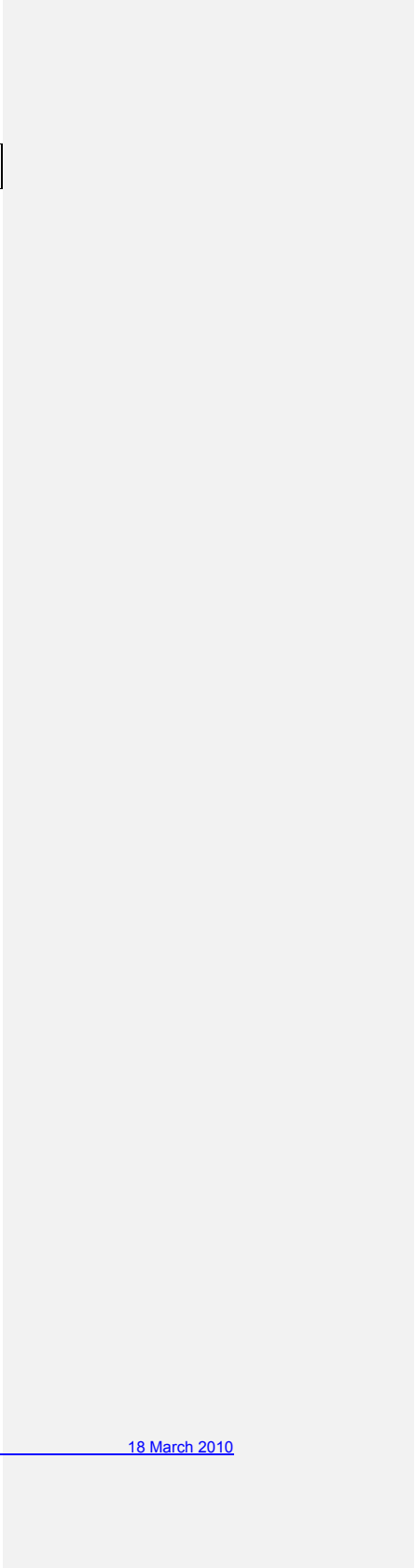
**1112 Destroy**  
**In: uuidKey**  
  
Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f  
  
 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040  
 000000000000042000D020000000400000001000000004200F010000004842005C05000000040000000140000000042  
 00790100000030420094070000002430643535323136302D666230342D346637632D386137332D6665663930356232316  
 33066000000000

**Out: uuidKey**  
  
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B751FB4 (Fri Feb 12 10:30:28 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f  
  
 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040  
 0000000000000420092090000008000000004B751FB44200D02000000400000001000000004200F010000005842

<a href="#">005C0500000040000014000000042007F0500000040000000000000042007C01000003042009407000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000</a>
--

243

244



245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264

## 11 Implementation Conformance

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

## 11 Access Control, Policies

[These use-cases test attributes and objects related to access control and server policy.](#)

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

[Pass a Credential object in the message header in all requests for identification purposes \(how the Credential object is used is defined in \[KMIP-Prof\]\). Create a symmetric key and set the Operation Policy Name attribute to "default". Using another Credential, attempt to perform a Get operation batched with a Get Attribute List on the created symmetric key – according to the Default Operation Policy, both these request SHALL fail, and with the Batch Error Continuation Option set to "Continue", the client SHALL also receive both response payloads. Using the initially used Credential, destroy the object and get the Destroy Date attribute.](#)

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

Time	Request/Response
0	<p><a href="#">Create (symmetric key)</a></p> <p><a href="#">In (header): credential={ credentialType='1', credentialValue={ username="Fred", password="password1" } }</a></p> <p><a href="#">In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='PolicyKey', NameType='00000001' }, OperationPolicyName='default', CryptographicParameters={ BlockCipherMode='1', PaddingMethod='3', HashingAlgorithm='4' }</a></p> <p><a href="#">Tag: Request Message (0x420078), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Request Header (0x420077), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</a></p> <p><a href="#">Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</a></p> <p><a href="#">Tag: Authentication (0x42000C), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Credential (0x420023), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password)</a></p> <p><a href="#">Tag: Credential Value (0x420025), Type: Structure (0x01), Data:</a></p> <p><a href="#">Tag: Username (0x420099), Type: Text String (0x07), Data: Fred</a></p> <p><a href="#">Tag: Password (0x4200A1), Type: Text String (0x07), Data: password1</a></p> <p><a href="#">Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</a></p> <p><a href="#">Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</a></p>

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm  
Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length  
Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage  
Mask  
Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name  
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:  
Tag: Name Value (0x420055), Type: Text String (0x07), Data: PolicyKey  
Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Operation Policy Name  
Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: default  
Tag: Attribute (0x420008), Type: Structure (0x01), Data:  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic  
Parameters  
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:  
Tag: Block Cipher Mode (0x420011), Type: Enumeration (0x05), Data: 0x00000001 (CBC)  
Tag: Padding Method (0x42005F), Type: Enumeration (0x05), Data: 0x00000003 (PKCS5)  
Tag: Hashing Algorithm (0x420038), Type: Enumeration (0x05), Data: 0x00000004 (SHA-1)

42007801000002504200770100000088420069010000002042006A0200000004000000010000000042006B0200000004000000000042000C010000004842002301000000404200240500000004000000010000000042002501000000028420099070000000446726564000000004200A107000000970617373776F726431000000000000042000D02000000040000000000042000F01000001B842005C050000004000000010000000042007901000001A0420057050000004000000200000000420091010000018842000801000000304200A070000001743727970746F6772617068696320416C676F726974686D004200B0500000040000000300000004200801000000304200A070000001443727970746F67726170686963204C656E67746800000004200B0200000040000008000000004200801000000304200A070000001843727970746F67726170686963205573616765204D61736B4200B0200000040000000C00000004200801000000404200A0700000044E616D50000004200B0100000028420055070000009506F6C6963794B6579000000000004200540500000040000000100000004200801000000304200A07000000154F7065726174696F6E20506F6C696379204E616D65000004200B07000000764656661756C740042000801000000584200A070000001843727970746F6772617068696320506172616D65746572734200B01000000304200110500000040000001000000042005F0500000040000000300000042003805000000400000040000000

Out: objectType='00000002', uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B9F8B4B (Tue Mar 16

	<p>14:44:43 CET 2010)</p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)</u></p> <p><u>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</u></p> <p><u>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b</u></p> <p>42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000420092090000000800000004B9F8B4B42000D020000004000000010000000042000F010000006842005C0500000004000000010000000042007F05000000040000000000000042007C0100000040420057050000000400000000000000420094070000002436333437383631352D386236642D346337302D626332332D38643136343831373535356200000000</p>
1	<p><u>Client A</u></p> <p><u>Get Attributes, Get</u></p> <p><u>In (header): credential={ credentialType='1', credentialValue={ username="Fred", password="password" }}</u></p> <p><u>In: attributeName='Operation Policy Name'</u></p> <p><u>In: uuidKey</u></p> <p><u>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</u></p> <p><u>Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</u></p> <p><u>Tag: Authentication (0x42000C), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Credential (0x420023), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password)</u></p> <p><u>Tag: Credential Value (0x420025), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Username (0x420099), Type: Text String (0x07), Data: Fred</u></p> <p><u>Tag: Password (0x4200A1), Type: Text String (0x07), Data: password1</u></p> <p><u>Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)</u></p> <p><u>Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 4CBB6751574C4DA8</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b</u></p> <p><u>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Operation Policy Name</u></p> <p><u>Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)</u></p> <p><u>Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 0EA05EE703DA997B</u></p> <p><u>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</u></p> <p><u>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b</u></p> <p>42007801000001704200770100000088420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000C0100000048420023010000004042002405000000040000000100000000420025010000002842</p>

00990700000044672656400000004200A107000000970617373776F7264310000000000004200D0200000004000  
0000200000004200F010000007842005C0500000040000000B0000000042009308000000084CBB6751574C4DA84200  
790100000050420094070000002436333437383631352D386236642D346337302D626332332D386431363438313735353  
562000000004200A07000000154F7065726174696F6E20506F6C696379204E616D6500000042000F010000005842005C  
0500000004000000A0000000042009308000000080EA05EE703DA997B420079010000003042009407000000243633343  
7383631352D386236642D346337302D626332332D3864313634383137353535620000000

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

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

42007B010000001b842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040  
00000000000004200920900000008000000004B9F8B4C4200D0200000040000000200000004200F01000000A042  
005C0500000040000000B0000000042009308000000084CBB6751574C4DA842007F05000000400000000000000420  
07C0100000068420094070000002436333437383631352D386236642D346337302D626332332D386431363438313735353  
356200000004200A070000003042000A07000000154F7065726174696F6E20506F6C696379204E616D6500000042000  
B070000000764656661756C740042000F01000000D842005C050000004000000A000000004200930800000080EA05E  
E703DA997B42007F0500000040000000000000042007C01000000A04200570500000040000000200000004200940  
70000002436333437383631352D386236642D346337302D626332332D386431363438313735353562000000042008F01



	<p>0000005842004001000000504200420500000004000000010000000042004501000000184200430800000010C520FCA4E681F7BFFB3523D71427D5944200280500000004000000030000000042002A02000000040000008000000000</p>
2	<p><b>Client B</b>  <a href="#">Get (symmetric key), Get Attribute List</a>  In (header): credential={ credentialType='1', credentialValue={ username="Barney", password="secret2" } }, BatchOrderOption='true', BatchErrorContinuationOption='Continue'  In: uuidKey  In: uuidKey</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:  Tag: Request Header (0x420077), Type: Structure (0x01), Data:  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  Tag: Authentication (0x42000C), Type: Structure (0x01), Data:  Tag: Credential (0x420023), Type: Structure (0x01), Data:  Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password)  Tag: Credential Value (0x420025), Type: Structure (0x01), Data:  Tag: Username (0x420099), Type: Text String (0x07), Data: Barney  Tag: Password (0x4200A1), Type: Text String (0x07), Data: secret2  Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE  Tag: Batch Error Continuation Option (0x42000E), Type: Enumeration (0x05), Data: 0x00000001  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: E3E72D5A352687D8  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)  Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: A9A1D60B0C62ECAF  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b</p> <p>420078010000016842007701000000A0420069010000002042006A0200000004000000010000000042006B020000000400000000000042000C01000000404200230100000038420024050000000400000001000000004200250100000002042009907000000064261726E657900004200A107000000077365637265743200420010060000000800000000000000000000142000E0500000004000000010000000042000D0200000004000000020000000042000F0100000005842005C05000000040000000A000000004200930800000008E3E72D5A352687D84200790100000030420094070000002436333437383631352D386236642D346337302D62633232D386431363438313735353562000000042000F010000005842005C05000000040000000C0000000004200930800000008A9A1D60B0C62ECAF4200790100000030420094070000002436333437383631352D386236642D346337302D626332332D38643136343831373535356200000000</p> <p><a href="#">Out: Operation Failed, Permission Denied</a>  <a href="#">Out: Operation Failed, Permission Denied</a></p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</p>

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

42007B010000011042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000004200920900000008000000004B9F8B4D42000D0200000004000000020000000042000F010000005842005C05000000040000000A000000004200930800000008E3E72D5A352687D842007F0500000004000000010000000042007E05000000040000000C0000000042007D070000000D4163636573732064656E69656400000042000F010000005842005C05000000040000000C000000004200930800000008A9A1D60B0C62ECAF42007F0500000004000000010000000042007E05000000040000000C0000000042007D070000000D4163636573732064656E696564000000

**3** Destroy  
In (header): credential={ credentialType='1', credentialValue={ username="Fred", password="password1" }}  
In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Authentication (0x42000C), Type: Structure (0x01), Data:  
Tag: Credential (0x420023), Type: Structure (0x01), Data:  
Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password)  
Tag: Credential Value (0x420025), Type: Structure (0x01), Data:  
Tag: Username (0x420099), Type: Text String (0x07), Data: Fred  
Tag: Password (0x4200A1), Type: Text String (0x07), Data: password1  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b

42007801000000E04200770100000088420069010000002042006A0200000004000000010000000042006B02000000040

000000000000042000C01000000484200230100000040420024050000004000000010000000420025010000002842  
0099070000000446726564000000004200A1070000000970617373776F726431000000000000042000D020000004000  
000010000000042000F010000004842005C0500000004000000140000000420079010000003042009407000000243633  
3437383631352D386236642D346337302D626332332D38643136343831373535356200000000

Out: uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B9F8B4D (Tue Mar 16 14:44:45 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040  
000000000000004200920900000008000000004B9F8B4D42000D0200000004000000010000000042000F010000005842  
005C0500000004000000140000000042007F05000000040000000000000042007C01000000304200940700000024363  
3437383631352D386236642D346337302D626332332D38643136343831373535356200000000

4

Get Attributes

In (header): credential={ credentialType='1', credentialValue={ username="Fred", password="password1" }}  
In: uuidKey, attributeNames={ 'Destroy Date' }

Tag: Request Message (0x420078), Type: Structure (0x01), Data:  
Tag: Request Header (0x420077), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Authentication (0x42000C), Type: Structure (0x01), Data:  
Tag: Credential (0x420023), Type: Structure (0x01), Data:  
Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password)  
Tag: Credential Value (0x420025), Type: Structure (0x01), Data:  
Tag: Username (0x420099), Type: Text String (0x07), Data: Fred  
Tag: Password (0x4200A1), Type: Text String (0x07), Data: password1  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b  
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Destroy Date

42007801000000F84200770100000088420069010000002042006A0200000004000000010000000042006B0200000040  
 0000000000000042000C010000004842002301000000404200240500000004000000010000000420025010000002842  
 0099070000000446726564000000004200A1070000000970617373776F726431000000000000042000D0200000004000  
 000010000000042000F010000006042005C05000000040000000B00000000420079010000004842009407000000243633  
 3437383631352D386236642D346337302D626332332D3864313634383137353535620000000042000A070000000C44657  
 374726F79204461746500000000

[Out: uuidKey, attributes={ DestroyDate=' 0x000000004B9F8B4D' }](#)

[Tag: Response Message \(0x42007B\), Type: Structure \(0x01\), Data:](#)

[Tag: Response Header \(0x42007A\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version \(0x420069\), Type: Structure \(0x01\), Data:](#)

[Tag: Protocol Version Major \(0x42006A\), Type: Integer \(0x02\), Data: 0x00000001 \(1\)](#)

[Tag: Protocol Version Minor \(0x42006B\), Type: Integer \(0x02\), Data: 0x00000000 \(0\)](#)

[Tag: Time Stamp \(0x420092\), Type: Date-Time \(0x09\), Data: 0x000000004B9F8B4E \(Tue Mar 16 14:44:46 CET 2010\)](#)

[Tag: Batch Count \(0x42000D\), Type: Integer \(0x02\), Data: 0x00000001 \(1\)](#)

[Tag: Batch Item \(0x42000F\), Type: Structure \(0x01\), Data:](#)

[Tag: Operation \(0x42005C\), Type: Enumeration \(0x05\), Data: 0x0000000B \(Get Attributes\)](#)

[Tag: Result Status \(0x42007F\), Type: Enumeration \(0x05\), Data: 0x00000000 \(Success\)](#)

[Tag: Response Payload \(0x42007C\), Type: Structure \(0x01\), Data:](#)

[Tag: Unique Identifier \(0x420094\), Type: Text String \(0x07\), Data: 63478615-8b6d-4c70-bc23-8d164817555b](#)

[Tag: Attribute \(0x420008\), Type: Structure \(0x01\), Data:](#)

[Tag: Attribute Name \(0x42000A\), Type: Text String \(0x07\), Data: Destroy Date](#)

[Tag: Attribute Value \(0x42000B\), Type: Date-Time \(0x09\), Data: 0x000000004B9F8B4D \(Tue Mar 16 14:44:45 CET 2010\)](#)

42007B01000000E042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040  
 000000000000004200920900000008000000004B9F8B4E42000D0200000004000000010000000042000F0100000008842  
 005C05000000040000000B0000000042007F050000000400000000000000000042007C010000000604200940700000024363  
 3437383631352D386236642D346337302D626332332D3864313634383137353535620000000042000801000000284200  
 0A070000000C44657374726F7920446174650000000042000B0900000008000000004B9F8B4D

265

266

267 **[12 Query, Maximum Response Size](#)**

268

269 [This use case tests the Query operation and the Maximum Response Size header field.](#)

270 **[12.1 Use-case: Query, Maximum Response Size](#)**

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

275

<a href="#">Time</a>	<a href="#">Request/Response</a>
<a href="#">0</a>	<a href="#">Query (operations, objects)</a> <a href="#">In (header): maximumResponseSize='256'</a>

In: queryFunctions={ '0000001', '0000002' }

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Maximum Response Size (0x420050), Type: Integer (0x02), Data: 0x00000100 (256)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000018 (Query)

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

Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000001 (Operations)

Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000002 (Objects)

42007801000000904200770100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000042005002000000400000100000000042000D02000000400000010000000042000F010000003842005C0500000040000001800000000420079010000002042007405000000400000010000000420074050000004000000000

Out: Operation Failed, Response Too Large

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B7918AA (Mon Feb 15 10:49:30 CET 2010)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)

Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x00000002 (Response Too Large)

Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Response size: 568, Maximum Response Size indicated in request: 256

Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000000 (0)

42007B01000000C042007A01000000B8420069010000002042006A0200000004000000010000000042006B0200000004000000000000420092090000000800000004B7918AA42007F0500000004000000010000000042007E050000000400000020000000042007D0700000043526573706F6E73652073697A653A203536382C204D6178696D756D20526573706F6E73652053697A6520696E6469636174656420696E20726571756573743A20323536000000000042000D0200000040000000000000

1

Query (operations, objects)

In (header): maximumResponseSize='2048'

In: queryFunctions={ '0000001', '0000002' }

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Maximum Response Size (0x420050), Type: Integer (0x02), Data: 0x00000800 (2048)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000018 (Query)  
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:  
Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000001 (Operations)  
Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000002 (Objects)

42007801000000904200770100000048420069010000002042006A0200000004000000010000000042006B02000000040  
000000000000004200500200000004000008000000000042000D0200000004000000010000000042000F010000003842  
005C050000000400000018000000004200790100000020420074050000000400000001000000004200740500000004000  
00002000000000

### Out: operations, objects

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:  
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:  
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:  
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)  
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B7918AA (Mon Feb 15 10:49:30 CET 2010)  
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)  
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000018 (Query)  
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)  
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000002 (Create Key Pair)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000009 (Check)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000012 (Activate)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000015 (Archive)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000016 (Recover)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000018 (Query)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000019 (Cancel)  
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll)

Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Certificate)  
Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)  
Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000003 (Public Key)  
Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000004 (Private Key)  
Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000006 (Template)

42007B010000023042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040  
0000000000000004200920900000008000000004B7918AA42000D0200000004000000010000000042000F01000001D842  
005C0500000004000000180000000042007F050000000400000000000000042007C01000001B042005C0500000004000  
000010000000042005C0500000004000000020000000042005C0500000004000000030000000042005C05000000040000  
00040000000042005C0500000004000000080000000042005C0500000004000000090000000042005C0500000004000000  
00A0000000042005C05000000040000000B0000000042005C05000000040000000C0000000042005C0500000004000000  
0D0000000042005C05000000040000000E0000000042005C05000000040000000F0000000042005C050000000400000001  
00000000042005C0500000004000000110000000042005C0500000004000000120000000042005C050000000400000013  
0000000042005C0500000004000000140000000042005C0500000004000000150000000042005C0500000004000000160  
000000042005C0500000004000000180000000042005C0500000004000000190000000042005C05000000040000001A00  
0000004200570500000004000000010000000042005705000000040000000200000000420057050000000400000003000  
000004200570500000004000000040000000042005705000000040000000600000000

277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328

## A. Acknowledgments

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

### Original Authors of the initial contribution:

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

### Participants:

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

Formatted: Heading 1,h1,Level 1 Topic Heading, Outline numbered + Level: 1 + Numbering Style: A, B, C, ... + Start at: 1 + Alignment: Left + Aligned at: 0 pt + Tab after: 21.6 pt + Indent at: 21.6 pt, Don't adjust space between Latin and Asian text

Formatted: Indent: First line: 36 pt



329 | Wyllys Ingersoll, [Sun MicrosystemsOracle Corporation](#)  
330 | Jay Jacobs, Target Corporation  
331 | Glen Jaquette, IBM  
332 | Scott Kipp, Brocade Communications Systems, Inc.  
333 | David Lawson, Emulex Corporation  
334 | [Hal Lockhart, Oracle Corporation](#)  
335 | Robert Lockhart, Thales e-Security  
336 | Shyam Mankala, EMC Corporation  
337 | [Upendra Mardikar, PayPal Inc.](#)  
338 | Marc Massar, Individual  
339 | Don McAlister, Associate  
340 | Hyrum Mills, Mitre Corporation  
341 | [Bob Nixon, Emulex Corporation](#)  
342 | Landon [Curt Noll](#), Cisco Systems, Inc.  
343 | René Pawlitzek, IBM  
344 | Rob Philpott, EMC Corporation  
345 | [Scott Rea, Individual](#)  
346 | Bruce Rich, IBM  
347 | Scott Rotondo, [Sun MicrosystemsOracle Corporation](#)  
348 | [Saikat Saha, Vormetric, Inc.](#)  
349 | Anil Saldhana, Red Hat  
350 | Subhash Sankuratripati, NetApp  
351 | Mark Schiller, [HPHewlett-Packard](#)  
352 | Jitendra Singh, Brocade Communications Systems, Inc.  
353 | Servesh Singh, EMC Corporation  
354 | [Terence Spies, Voltage Security](#)  
355 | Sandy Stewart, [Sun MicrosystemsOracle Corporation](#)  
356 | Marcus Streets, Thales e-Security  
357 | Brett Thompson, SafeNet, Inc.  
358 | Benjamin Tomhave, Individual  
359 | Sean Turner, IECA, Inc.  
360 | Paul Turner, Venafi, Inc.  
361 | Marko [Vukolić](#), IBM  
362 | Rod Wideman, Quantum Corporation  
363 | Steven Wierenga, [HPHewlett-Packard](#)  
364 | Peter Yee, EMC Corporation  
365 | Krishna Yellepeddy, IBM  
366 | Peter Zelechowski, [Associate](#)

367  
368

369

## B. Revision History

Revision	Date	Editor	Changes Made
ed-0.98	2009-04-28	Mathias Björkqvist	Initial conversion of input document to OASIS format.
ed-0.98	2009-08-06	Mathias Björkqvist	Changes to layout and message content to reflect the recent changes to the KMIP specification, added descriptions to the use-cases for which they were missing.
ed-0.98	2009-09-28	Mathias Björkqvist	Updated messages and TTLV encodings to conform with KMIP specification ed-0.98 rev 17.
draft-01	2009-10-08	Mathias Björkqvist	Removed normative words “must”, “shall”, “required”, “will” and “can”; updated messages and TTLV encodings to conform to KMIP specification ed-0.98 rev 19; added normative references; added minor edits
draft-02	2009-10-15	Mathias Björkqvist	Replaced the TBDs, changed status to Committee Draft, changed use-cases to use protocol major version 1 and minor version 0
draft-03	2009-10-15	Mathias Björkqvist	Corrected names of TC chairs
draft-04	2009-11-05	Mathias Björkqvist	Added list of participants, added reference to Profiles document, line spacing change to list of original contributors, added related documents
cd-05	2009-11-06	Mathias Björkqvist	Changes to various naming aspects on front page and document footer. This is the tentative version for public review.

370

<a href="#">cd-06</a>	<a href="#">2009-11-12</a>	<a href="#">Mathias Björkqvist</a>	<a href="#">Updated tags.</a>
<a href="#">cd-07</a>	<a href="#">2010-02-17</a>	<a href="#">Mathias Björkqvist</a>	<a href="#">Addressed public review comments, added line numbering.</a>
<a href="#">cd-08</a>	<a href="#">2010-03-17</a>	<a href="#">Mathias Björkqvist</a>	<a href="#">Registration of Templates changed to use the Template object. Usage Allocation changes (Add Attribute, Check, Get Usage Allocation), batched Revoke requests with Destroy requests when destroying objects in the Active state, adopted new format for Username and Password Credential object.</a>
<a href="#">cd-09</a>	<a href="#">2010-03-18</a>	<a href="#">Mathias Björkqvist</a>	<a href="#">Updated participants' list. Editorial fixes.</a>

371

Formatted

Formatted: Style Heading 1h1Level 1 Topic Heading + Before: 5 pt After: 5..., Outline numbered + Level: 1 + Numbering Style: A, B, C, ... + Start at: 1 + Alignment: Left + Aligned at: 0 pt + Tab after: 21.6 pt + Indent at: 21.6 pt

Page 4: [1] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [1] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [2] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [2] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [3] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [3] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [4] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [4] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [5] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [5] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [6] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [6] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [7] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [7] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [8] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [8] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [9] Change	Unknown
--------------------	---------

Field Code Changed

Page 4: [10] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [10] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [11] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [11] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [12] Formatted	subhash	4/14/2010 5:02:00 PM
------------------------	---------	----------------------

Don't adjust space between Latin and Asian text, Tab stops: Not at 48 pt

Page 4: [13] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [13] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [14] Formatted	subhash	4/14/2010 5:02:00 PM
------------------------	---------	----------------------

Don't adjust space between Latin and Asian text, Tab stops: Not at 24 pt

Page 4: [15] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [15] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [16] Formatted	subhash	4/14/2010 5:02:00 PM
------------------------	---------	----------------------

Don't adjust space between Latin and Asian text, Tab stops: Not at 48 pt

Page 4: [17] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [17] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [18] Formatted	subhash	4/14/2010 5:02:00 PM
------------------------	---------	----------------------

Don't adjust space between Latin and Asian text, Tab stops: Not at 24 pt

Page 4: [19] Change	Unknown
---------------------	---------

Field Code Changed

Field Code Changed

Page 4: [20] Formatted	subhash	4/14/2010 5:02:00 PM
------------------------	---------	----------------------

Don't adjust space between Latin and Asian text, Tab stops: Not at 48 pt

Page 4: [21] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [21] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [22] Formatted	subhash	4/14/2010 5:02:00 PM
------------------------	---------	----------------------

Don't adjust space between Latin and Asian text, Tab stops: Not at 24 pt

Page 4: [23] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [23] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [24] Formatted	subhash	4/14/2010 5:02:00 PM
------------------------	---------	----------------------

Don't adjust space between Latin and Asian text, Tab stops: Not at 48 pt

Page 4: [25] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [25] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [26] Change	Unknown
---------------------	---------

Field Code Changed

Page 4: [26] Change	Unknown
---------------------	---------

Field Code Changed