



Key Management Interoperability Protocol Use Cases Version 1.0

Committee Draft 09 / Public Review 02

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

Latest Version:

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

Technical Committee:

OASIS Key Management Interoperability Protocol (KMIP) TC

Chair(s):

Robert Griffin, EMC Corporation <robert.griffin@rsa.com>
Subhash Sankuratripati, NetApp <Subhash.Sankuratripati@netapp.com>

Editor(s):

Mathias Björkqvist, IBM <mbj@zurich.ibm.com>
René Pawlitzek, IBM <rpa@zurich.ibm.com>

Related work:

This specification replaces or supersedes:

- None

This specification is related to:

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

Abstract:

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

Status:

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

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

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

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

Notices

Copyright © OASIS® 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", [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	Table of Contents	4
2		
3	1 Introduction	5
4	1.1 Normative References	5
5	2 Message exchange	5
6	3 Centralized Management	5
7	3.1 Basic functionality	5
8	3.1.1 Use-case: Create / Destroy	6
9	3.1.2 Use-case: Register / Create / Get attributes / Destroy	8
10	3.1.3 Use-case: Create / Locate / Get / Destroy	14
11	3.1.4 Use-case: Dual client use-case, ID Placeholder linked Locate & Get batch	19
12	3.1.5 Use-case: Register / Destroy Secret Data	33
13	3.2 Use-case: Asynchronous Locate	35
14	4 Key life cycle support	45
15	4.1 Use-case: Revoke scenario	46
16	5 Auditing and reporting	62
17	5.1 Use-case: Get usage allocation scenario	62
18	6 Key Interchange, Key Exchange	75
19	6.1 Use-case: Import of a Third-party Key	75
20	7 Vendor Extensions	79
21	7.1 Use-case: Unrecognized Message Extension with Criticality Indicator false	80
22	7.2 Use-case: Unrecognized Message Extension with Criticality Indicator true	82
23	8 Asymmetric keys	83
24	8.1 Use-case: Create a Key Pair	83
25	8.2 Use-case: Register Both Halves of a Key Pair	89
26	9 Key Roll-over	97
27	9.1 Use-case: Create a Key, Re-key	97
28	9.2 Use-case: Existing Key Expired, Re-key with Same lifecycle	104
29	9.3 Use-case: Existing Key Compromised, Re-key with same lifecycle	114
30	9.4 Use-case: Create key, Re-key with new lifecycle	122
31	9.5 Use-case: Obtain Lease for Expired Key	131
32	10 Archival	142
33	10.1 Use-case: Create a Key, Archive and Recover it	142
34	11 Access Control, Policies	155
35	11.1 Use-case: Credential, Operation Policy, Destroy Date	155
36	12 Query, Maximum Response Size	162
37	12.1 Use-case: Query, Maximum Response Size	162
38	A. Acknowledgments	166
39	B. Revision History	167
40		

41 1 Introduction

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

48
49 The use-cases define a number of client-to-server request-response pairs for a number of operations. For
50 each request-response message pair the operation is stated, along with the relevant parameters needed
51 for the request or response message. This is followed by two different illustrations of the messages: first,
52 a human-readable construction which shows the fields tags, types and values, followed by the TTLV-
53 encoding of the message. These are included to facilitate the implementation of the message creation
54 and parsing functionality. The use-cases show one possible way to construct the messages, and the
55 messages shown are not necessarily the only correct constructions (e.g. it is possible to omit the attribute
56 index if it is zero). Also note that many values change dynamically when running the use-cases (the
57 server-generated timestamps, Unique Identifiers and key material in responses, as well as Batch Item ID
58 values in client-generated requests).

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

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

68 1.1 Normative References

- 69 **[KMIP-Spec]** OASIS Committee Draft 06, *Key Management Interoperability Protocol*
70 *Specification Version 1.0*, Nov 2009,
71 <http://docs.oasis-open.org/kmip/spec/v1.0/cd06/kmip-spec-1.0-cd-06.doc>
72 **[KMIP-Prof]** OASIS Committee Draft 04, *Key Management Interoperability Protocol Profiles*
73 *Version 1.0*, Nov 2009,
74 <http://docs.oasis-open.org/kmip/profiles/v1.0/cd04/kmip-profiles-1.0-cd-04.doc>
75

76 2 Message exchange

77 The message exchange between clients and the server to test the following use-case scenarios is
78 performed with TTLV encoding over the TLS/SSL transport as defined in **[KMIP-Spec]** and **[KMIP-Prof]**.
79

80 3 Centralized Management

81 3.1 Basic functionality

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

85 **3.1.1 Use-case: Create / Destroy**

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

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 (0x420078), Type: Structure (0x01), Data:</p> <ul style="list-style-type: none"> Tag: Request Header (0x420077), Type: Structure (0x01), Data: <ul style="list-style-type: none"> Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: <ul style="list-style-type: none"> Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: <ul style="list-style-type: none"> Tag: Attribute (0x420008), Type: Structure (0x01), Data: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt) <p>42007801000001204200770100000038420069010000002042006A0200000004000000010000000042006B0200000004 000000000000000042000D0200000004000000010000000042000F01000000D842005C05000000040000000100000000 42007901000000C04200570500000004000000020000000042009101000000A8420008010000003042000A0700000017 43727970746F6772617068696320416C676F726974686D0042000B050000000400000003000000004200080100000030 42000A070000001443727970746F67726170686963204C656E677468000000042000B02000000040000008000000000 420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004 0000000C00000000</p> <p>Out: objectType='00000002', uuidKey</p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</p> <ul style="list-style-type: none"> Tag: Response Header (0x42007A), Type: Structure (0x01), Data: <ul style="list-style-type: none"> Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C2 (Thu Nov 12 11:47:30 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fc8833de-70d2-4ece-b063-fede3a3c59fe

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004
 00000000000000004200920900000008000000004AFBE7C242000D0200000004000000010000000042000F0100000068
 42005C0500000004000000010000000042007F05000000040000000000000042007C01000000404200570500000004
 0000000200000000420094070000002466633838333364652D373064322D346563652D623036332D6665646533613363
 3539666500000000

1
Destroy (symmetric key)
In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fc8833de-70d2-4ece-b063-fede3a3c59fe

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004
 000000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000001400000000
 4200790100000030420094070000002466633838333364652D373064322D346563652D623036332D6665646533613363
 3539666500000000

Out: uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C3 (Thu Nov 12 11:47:31 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

	<p>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)</p> <p>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</p> <p style="padding-left: 20px;">Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fc8833de-70d2-4ece-b063-fede3a3c59fe</p> <p>42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBE7C342000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002466633838333364652D373064322D346563652D623036332D66656465336133633539666500000000</p>
--	--

89

90

91 **3.1.2 Use-case: Register / Create / Get attributes / Destroy**

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

95

Time	Request/Response messages
0	<p>Register (template)</p> <p>In: objectType='00000007', TemplateAttribute=empty, Template={ ObjectGroup='Group1', ApplicationSpecificInformation='ssl, www.example.com', ContactInformation='Joe', x-Purpose='demonstration', Name={ NameValue='Template1', NameType='00000001' } }</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</p> <p style="padding-left: 20px;">Tag: Request Header (0x420077), Type: Structure (0x01), Data:</p> <p style="padding-left: 40px;">Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:</p> <p style="padding-left: 60px;">Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p style="padding-left: 60px;">Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)</p> <p style="padding-left: 40px;">Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)</p> <p style="padding-left: 20px;">Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p style="padding-left: 40px;">Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)</p> <p style="padding-left: 20px;">Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p style="padding-left: 40px;">Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000006 (Template)</p> <p style="padding-left: 40px;">Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: null</p> <p style="padding-left: 40px;">Tag: Template (0x420090), Type: Structure (0x01), Data:</p> <p style="padding-left: 60px;">Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p style="padding-left: 80px;">Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group</p> <p style="padding-left: 80px;">Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1</p> <p style="padding-left: 60px;">Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p style="padding-left: 80px;">Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Application Specific Information</p> <p style="padding-left: 80px;">Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:</p> <p style="padding-left: 100px;">Tag: Application Namespace (0x420003), Type: Text String (0x07), Data: ssl</p> <p style="padding-left: 100px;">Tag: Application Data (0x420002), Type: Text String (0x07), Data: www.example.com</p> <p style="padding-left: 60px;">Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p style="padding-left: 80px;">Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information</p> <p style="padding-left: 80px;">Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe</p> <p style="padding-left: 60px;">Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p>

Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-Purpose
 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: demonstration
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
 Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
 Tag: Name Value (0x420055), Type: Text String (0x07), Data: Template1
 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

```
42007801000001C84200770100000038420069010000002042006A020000000400000001000000042006B02000000040
00000000000000042000D020000000400000001000000042000F010000018042005C0500000004000000030000000042
0079010000016842005705000000040000000600000000420091010000000042009001000001484200080100000028420
00A070000000C4F626A6563742047726F7570000000042000B070000000647726F757031000042000801000000584200
0A07000000204170706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000B010000002842000
3070000000373736C000000000420002070000000F7777772E6578616D706C652E636F6D00420008010000003042000A
0700000013436F6E7461637420496E666F726D6174696F6E00000000042000B07000000034A6F650000000004200080
10000003042000A0700000009782D507572706F7365000000000000042000B070000000D64656D6F6E7374726174696F
6E000000420008010000004042000A07000000044E616D65000000042000B0100000028420055070000000954656D706
C61746531000000000000042005405000000040000000100000000
```

Out: uuidTemplate

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C4 (Thu Nov 12 11:47:32 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a6ebbb6f-4c54-4bbb-ad29-be6bad4ecad5

```
42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040
000000000000004200920900000008000000004AFBE7C442000D0200000004000000010000000042000F010000005842
005C0500000004000000030000000042007F050000000400000000000000042007C01000000304200940700000024613
66562626236662D346335342D346262622D616432392D62653662616434656361643500000000
```

1	<p>Create (symmetric key using template)</p> <p>In: objectType='00000002', template={ NameValue='Template1', NameType='00000001' }, attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C' }</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:</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: Name (0x420053), Type: Structure (0x01), Data:
 - Tag: Name Value (0x420055), Type: Text String (0x07), Data: Template1
 - Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
 - Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 - Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
 - Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
 - Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 - Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
 - Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
 - Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 - Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage

Mask

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

```
42007801000001504200770100000038420069010000002042006A020000000400000001000000042006B02000000040
000000000000042000D02000000400000001000000042000F01000010842005C050000004000000010000000042
007901000000F0420057050000000400000002000000042009101000000D842005301000000284200550700000009546
56D706C617465310000000000000420054050000004000000010000000420008010000003042000A07000000174372
7970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000
A070000001443727970746F67726170686963204C656E677468000000042000B020000004000000800000000420008
010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000040000000
C00000000
```

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: 0x00000004AFBE7C5 (Thu Nov 12 11:47:33 CET 2009)
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
 - Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 - Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 - Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-2fa6eald747a

```
42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040
000000000000042009209000000800000004AFBE7C542000D02000000400000001000000042000F010000006842
005C050000000400000001000000042007F05000000040000000000000042007C01000000404200570500000004000
0000200000000420094070000002436316231303631342D643862352D343666392D386431372D32666136656131643734
376100000000
```

2	Get attributes
---	----------------

In: uuidKey, attributeNames={ 'ObjectGroup', 'ApplicationSpecificInformation', 'ContactInformation', 'x-Purpose' }

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
Tag: Request Header (0x420077), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-2fa6eald747a
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

42007801000001084200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F01000000C042005C05000000040000000B0000000042007901000000A8420094070000002436316231303631342D643862352D343666392D386431372D3266613665613164373437610000000042000A070000000C4F626A6563742047726F75700000000042000A07000000204170706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000A0700000013436F6E7461637420496E666F726D6174696F6E000000000042000A0700000009782D507572706F736500000000000000

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

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C6 (Thu Nov 12 11:47:34 CET 2009)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-2fa6eald747a
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

42007B01000001B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
 000000000000004200920900000008000000004AFBE7C642000D020000000400000001000000004200F010000015842
 005C050000000400000000B0000000042007F050000000400000000000000042007C01000001304200940700000024363
 16231303631342D643862352D343666392D386431372D3266613665613164373437610000000042000801000000284200
 0A070000000C4F626A6563742047726F75700000000042000B070000000647726F7570310000420008010000005842000
 A07000000204170706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000B0100000028420003
 070000000373736C0000000000420002070000000F7777772E6578616D706C652E636F6D00420008010000003042000A0
 700000013436F6E7461637420496E666F726D6174696F6E000000000042000B07000000034A6F65000000000042000801
 0000003042000A0700000009782D507572706F73650000000000000042000B070000000D64656D6F6E7374726174696F6E
 E000000

3

Destroy (symmetric key)

In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-2fa6eald747a

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
 0000000000000042000D020000000400000001000000004200F010000004842005C0500000004000000140000000042
 00790100000030420094070000002436316231303631342D643862352D343666392D386431372D3266613665613164373
 4376100000000

Out: uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C6 (Thu Nov 12 11:47:34 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

	<p>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-2fa6eald747a</p> <p>42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBE7C642000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002436316231303631342D643862352D343666392D386431372D32666136656131643734376100000000</p>
4	<p>Destroy (template)</p> <p>In: uuidTemplate</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: a6ebbb6f-4c54-4bbb-ad29-be6bad4ecad5</p> <p>42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002461366562626236662D346335342D346262622D616432392D62653662616434656361643500000000</p> <p>Out: uuidTemplate</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: 0x000000004AFBE7C6 (Thu Nov 12 11:47:34 CET 2009)</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: a6ebbb6f-4c54-4bbb-ad29-be6bad4ecad5</p> <p>42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBE7C642000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002461366562626236662D346335342D346262622D616432392D62653662616434656361643500000000</p>

98 **3.1.3 Use-case: Create / Locate / Get / Destroy**

99 This use-case tests the Locate and Get operations, in addition to the previously used operations Create
 100 and Destroy. A symmetric key is first created, and then a lookup is performed on the Name attribute using
 101 the Locate operation. Subsequently, a Get request is issued to retrieve the located key, after which the
 102 key on the server is destroyed.
 103

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 (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: 0x00000001 (Create)</p> <p> Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p> Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</p> <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: Name</p> <p> Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:</p> <p> Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1</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: Cryptographic Algorithm</p> <p> Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (3DES)</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: 0x000000A8 (168)</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: Contact Information</p> <p> Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe</p> <p>42007801000001984200770100000038420069010000002042006A0200000004000000010000000042006B02000000040 0000000000000042000D0200000004000000010000000042000F010000015042005C0500000004000000010000000042 00790100000138420057050000000400000002000000004200910100000120420008010000003842000A07000000044E6 16D650000000042000B010000002042005507000000044B657931000000042005405000000040000001000000004200 08010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B05000000040000 00200000000420008010000003042000A070000001443727970746F67726170686963204C656E677468000000042000B</p>

0200000004000000A800000000420008010000003042000A070000001843727970746F677261706869632055736167652
04D61736B42000B02000000040000000C00000000420008010000003042000A0700000013436F6E7461637420496E666F
726D6174696F6E000000000042000B07000000034A6F650000000000

Out: objectType = '00000002', uuidKey

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

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000040
000000000000004200920900000008000000004AFBE7C742000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F050000000400000000000000042007C01000000404200570500000004000
0000200000000420094070000002431656432386561352D326233312D343134352D626366322D33366430373536643338
393000000000

1

Locate (symmetric key)

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

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

42007801000000D04200770100000038420069010000002042006A0200000004000000010000000042006B020000000040

0000000000000042000D0200000004000000010000000042000F010000008842005C0500000004000000080000000042
00790100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000
0000200000000420008010000003842000A07000000044E616D650000000042000B010000002042005507000000044B65
793100000000042005405000000040000000100000000

Out: uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C8 (Thu Nov 12
11:47:36 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-
36d0756d3890

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004AFBE7C842000D0200000004000000010000000042000F010000005842
005C0500000004000000080000000042007F0500000004000000000000000042007C01000000304200940700000024316
56432386561352D326233312D343134352D626366322D33366430373536643338393000000000

2

Get (symmetric key)

In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-
36d0756d3890

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A0000000042
00790100000030420094070000002431656432386561352D326233312D343134352D626366322D3336643037353664333
83930000000000

Out: objectType = '00000002', uuidKey, symmetricKey

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

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C8 (Thu Nov 12 11:47:36 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890
 Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
 Tag: Key Block (0x420040), Type: Structure (0x01), Data:
 Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
 Tag: Key Value (0x420045), Type: Structure (0x01), Data:
 Tag: Key Material (0x420043), Type: Octet String (0x08), Data: C8E51523F73D6EE9F40EAB7CD06825499D8C0BD0739E1046
 Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000002 (3DES)
 Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x000000A8 (168)

42007B010000012842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000420092090000008000000004AFBE7C842000D0200000004000000010000000042000F01000000D042005C05000000040000000A0000000042007F05000000040000000000000042007C01000000A842005705000000040000000000000420094070000002431656432386561352D326233312D343134352D626366322D333664303735366433383930000000042008F01000000604200400100000058420042050000004000000010000000042004501000000204200430800000018C8E51523F73D6EE9F40EAB7CD06825499D8C0BD0739E1046420028050000004000000020000000042002A0200000004000000A800000000

3

Destroy (symmetric key)

In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000014000000004200790100000030420094070000002431656432386561352D326233312D343134352D626366322D33366430373536643338393000000000

Out: uuidKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

- Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
- Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C8 (Thu Nov 12 11:47:36 CET 2009)
- Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 - Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 - Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: led28ea5-2b31-4145-bcf2-36d0756d3890

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBE7C842000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F050000000400000000000000042007C0100000030420094070000002431656432386561352D326233312D343134352D626366322D33366430373536643338393000000000

4

Locate
In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

- Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
 - Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 - Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Unique Identifier
 - Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: led28ea5-2b31-4145-bcf2-36d0756d3890

42007801000000B84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000007042005C0500000004000000080000000004200790100000058420008010000005042000A0700000011556E69717565204964656E746966696572000000000000000042000B070000002431656432386561352D326233312D343134352D626366322D33366430373536643338393000000000

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:

<p>Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000008 (Locate)</p> <p>Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success)</p> <p>Tag: Response Payload (0x420079), Type: Structure (0x01), Data: null</p> <p>42007B010000008042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBE7C842000D0200000004000000010000000042000F010000002842005C0500000004000000080000000042007F0500000004000000000000000042007C0100000000</p>
--

104

105

106 **3.1.4 Use-case: Dual client use-case, ID Placeholder linked Locate & Get batch**

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

113

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

117

Time	Request/Response messages
0	<p>Client A:</p> <p>Register (template)</p> <p>In: objectType='00000007', TemplateAttribute=empty, Template={ CryptographicAlgorithm='AES', CryptographicLength='128', Name={ NameValue='Template1', 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: 0x00000003 (Register)</p> <p> Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p> Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000006 (Template)</p> <p> Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: null</p> <p> Tag: Template (0x420090), 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>

Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
 Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
 Tag: Name Value (0x420055), Type: Text String (0x07), Data: Template1
 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

```
42007801000001384200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F01000000F042005C0500000004000000030000000042
007901000000D8420057050000000400000006000000004200910100000000420090010000000B8420080100000030420
00A070000001743727970746F6772617068696320416C676F726974686D0042000B050000000400000003000000004200
08010000003042000A070000001443727970746F67726170686963204C656E677468000000042000B020000000400000
0800000000420008010000004042000A07000000044E616D65000000042000B0100000028420055070000000954656D
706C617465310000000000000042005405000000040000000100000000
```

Out: uuidTemplate

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED21 (Thu Nov 12 12:10:25 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 45d8629a-9ad1-41b3-9d09-941f2a595da3

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004AFBED2142000D0200000004000000010000000042000F010000005842
005C0500000004000000030000000042007F050000000400000000000000042007C01000000304200940700000024343
56438363239612D396164312D343162332D396430392D39343166326135393564613300000000
```

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

Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
 Tag: Name (0x420053), Type: Structure (0x01), Data:
 Tag: Name Value (0x420055), Type: Text String (0x07), Data: Templatel
 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
 Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
 Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
 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

Mask

```
42007801000001584200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000011042005C0500000004000000010000000042
007901000000F84200570500000004000000020000000042009101000000E042005301000000284200550700000009546
56D706C61746531000000000000042005405000000040000000100000000420008010000003842000A07000000044E61
6D650000000042000B010000002042005507000000044B657931000000004200540500000004000000010000000042000
8010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000
0400000000420008010000003042000A0700000013436F6E7461637420496E666F726D6174696F6E000000000042000B0
700000003466F6F0000000000
```

Out: objectType='00000002', uuidKey

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

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004AFBED2342000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F050000000400000000000000042007C01000000404200570500000004000
0000200000000420094070000002430613333653833652D356237612D343836352D393634612D386431633362663961
653300000000
```

2	Client B: Locate and Get (symmetric key by name)
---	---

In (header): batchOrderOption='TRUE'
In: attributes={ objectType = '00000002', Name={ Name='Key1', NameType='00000001'}}
In: <empty Get payload>

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 0E9E1875336E415E
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
 Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric
Key)
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
 Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
 Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: CFEF21DDDF1CF5E3
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: null

42007801000001204200770100000048420069010000002042006A0200000004000000010000000042006B020000000040
0000000000000042001006000000080000000000000142000D0200000004000000020000000042000F010000009842
005C05000000040000000800000000042009308000000080E9E1875336E415E42007901000000704200080100000028420
00A070000000B4F626A656374205479706500000000042000B0500000004000000020000000042000801000000384200
0A07000000044E616D650000000042000B010000002042005507000000044B65793100000000420054050000000400000
0010000000042000F010000002842005C05000000040000000A000000004200930800000008CFEF21DDDF1CF5E3420079
0100000000

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

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED24 (Thu Nov 12
12:10:28 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 0E9E1875336E415E
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: CFEF21DDDF1CF5E3
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
 Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
 Tag: Key Block (0x420040), Type: Structure (0x01), Data:
 Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
 Tag: Key Value (0x420045), Type: Structure (0x01), Data:
 Tag: Key Material (0x420043), Type: Octet String (0x08), Data:
 755D03C639648FB5828D5F1CC9FE9B57
 Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
 Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

42007B01000001A042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
 000000000000042009209000000800000004AFBED244200D0200000040000002000000042000F010000006842
 005C0500000004000000080000000042009308000000080E9E1875336E415E42007F050000000400000000000000420
 07C0100000030420094070000002430613333653833652D356237612D343836352D393634612D386431633362663961
 6533000000042000F01000000D842005C05000000040000000A000000004200930800000008CFEF21DDDF1CF5E342007
 F05000000040000000000000042007C01000000A04200570500000004000000200000004200940700000024306133
 33653833652D356237612D343836352D393634612D3864316333626639616533000000042008F01000000584200400
 1000000504200420500000040000001000000042004501000000184200430800000010755D03C639648FB5828D5F1C
 C9FE9B574200280500000004000000030000000042002A02000000040000008000000000

3

Client B:
Get attribute list
In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
 00000000000004200D0200000004000000010000000042000F010000004842005C05000000040000000C0000000042
 00790100000030420094070000002430613333653833652D356237612D343836352D393634612D38643163336266396
 16533000000000

Out: uuidKey, attributes={ * }

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED24 (Thu Nov 12 12:10:28 CET 2009)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digest
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Initial Date
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Unique Identifier
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Last Change Date

42007B01000001C842007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004AFBED2442000D0200000004000000010000000042000F010000017042005C05000000040000000C0000000042007F05000000040000000000000042007C0100000148420094070000002430613333653833652D356237612D343836352D393634612D3864316333626266396165330000000042000A0700000001443727970746F67726170686963204C656E677468000000042000A070000001743727970746F6772617068696320416C676F726974686D0042000A0700000005537461746500000042000A0700000006446967657374000042000A070000000C496E697469616C2044617465000000042000A0700000011556E69717565204964656E746966696572000000000000042000A07000000044E616D650000000042000A070000001843727970746F67726170686963205573616765204D61736B42000A070000000B4F626A656374205479706500000000042000A0700000013436F6E7461637420496E666F726D6174696F6E000000042000A07000000104C617374204368616E67652044617465

4

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
Tag: Request Header (0x420077), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)

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

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

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

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

42007801000000C04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000007842005C05000000040000000B000000004200790100000060420094070000002430613333653833652D356237612D343836352D393634612D386431633362626639616533000000042000A07000000044E616D65000000042000A0700000013436F6E7461637420496E666F726D6174696F6E0000000000

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

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED24 (Thu Nov 12 12:10:28 CET 2009)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

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

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

Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:

Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1

Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

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

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

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

42007B010000012842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000042009209000000800000004AFBED2442000D0200000004000000010000000042000F01000000D042005C05000000040000000B0000000042007F05000000040000000000000042007C01000000A8420094070000002430613333653833652D356237612D343836352D393634612D3864316333626266396165330000000420008010000003842000A07000000044E616D65000000042000B010000002042005507000000044B657931000000004200540500000004000000100000000420008010000003042000A0700000013436F6E7461637420496E666F726D6174696F6E00000000042000B0700000003466F6F0000000000

5	<p>Client B:</p> <p>Add attribute [batch]</p> <p>In: uuidKey, attribute={ x-attribute1='Value1' }</p> <p>In: uuidKey, attribute={ x-attribute2='Value2' }</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</p> <p>Tag: Request Header (0x420077), Type: Structure (0x01), Data:</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: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)

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

- Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
- Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7A92DDA525EB158A
- Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
 - Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 - Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
 - Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value1

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

- Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
- Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7230F6E4D3BEA249
- Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
 - Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 - Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
 - Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value2

```
42007801000001604200770100000038420069010000002042006A020000000400000001000000042006B02000000040
0000000000000042000D0200000004000000020000000042000F010000008842005C05000000040000000D0000000042
009308000000087A92DDA525EB158A4200790100000060420094070000002430613333653833652D356237612D3438363
52D393634612D3864316333626266396165330000000420008010000002842000A070000000C782D6174747269627574
65310000000042000B070000000656616C756531000042000F010000008842005C05000000040000000D0000000042009
308000000087230F6E4D3BEA2494200790100000060420094070000002430613333653833652D356237612D343836352D
393634612D3864316333626266396165330000000420008010000002842000A070000000C782D6174747269627574653
20000000042000B070000000656616C7565320000
```

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

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

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

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

Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value1
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7230F6E4D3BEA249
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value2

42007B010000019042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
 000000000000004200920900000008000000004AFBED2542000D0200000004000000020000000042000F010000009842
 005C05000000040000000D0000000042009308000000087A92DDA525EB158A42007F050000000400000000000000420
 07C010000006042009407000000243061333653833652D356237612D343836352D393634612D38643163336262663961
 6533000000042008010000002842000A070000000C782D617474726962757465310000000042000B070000000656616
 C756531000042000F010000009842005C05000000040000000D0000000042009308000000087230F6E4D3BEA24942007F
 050000000400000000000000042007C0100000006042009407000000243061333653833652D356237612D343836352D3
 93634612D3864316333626266396165330000000042008010000002842000A070000000C782D61747472696275746532
 0000000042000B070000000656616C7565320000

6

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BA3EA60548ECB699
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 321984E716274A3D
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2

42007801000001704200770100000038420069010000002042006A0200000004000000010000000042006B02000000040

0000000000000042000D0200000004000000020000000042000F010000009042005C05000000040000000E0000000042
009308000000008BA3EA60548ECB6994200790100000068420094070000002430613333653833652D356237612D3438363
52D393634612D3864316333626266396165330000000420008010000003042000A070000000C782D6174747269627574
65310000000042000B070000000E4D6F64696669656456616C756531000042000F010000009042005C050000000400000
00E00000000420093080000008321984E716274A3D4200790100000068420094070000002430613333653833652D3562
37612D343836352D393634612D3864316333626266396165330000000420008010000003042000A070000000C782D6174
47472696275746532000000042000B070000000E4D6F64696669656456616C7565320000

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

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

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED26 (Thu Nov 12 12:10:30 CET 2009)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BA3EA60548ECB699

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

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

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

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 321984E716274A3D

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

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

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

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

42007B01000001A042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000420092090000000800000004AFBED2642000D0200000004000000020000000042000F01000000A042
005C05000000040000000E00000000420093080000008BA3EA60548ECB69942007F050000000400000000000000420
07C0100000068420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961
653300000000420008010000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F6
4696669656456616C756531000042000F01000000A042005C05000000040000000E00000000420093080000008321984
E716274A3D42007F05000000040000000000000042007C0100000068420094070000002430613333653833652D35623
7612D343836352D393634612D3864316333626266396165330000000420008010000003042000A070000000C782D6174
47472696275746532000000042000B070000000E4D6F64696669656456616C7565320000

7	<p>Client B: Delete attribute [batch] In: uuidKey, attributeNames={'x-attribute1'}</p>
---	--

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
Tag: Request Header (0x420077), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D5C6DF842DAEECD8
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 572D4F0D433DAB10
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2

42007801000001304200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000042000D02000000400000002000000042000F010000007042005C05000000040000000F000000004200930800000008D5C6DF842DAEECD84200790100000048420094070000002430613333653833652D356237612D343836352D393634612D386431633362626639616533000000042000A070000000C782D617474726962757465310000000042000F010000007042005C05000000040000000F000000004200930800000008572D4F0D433DAB1042007901000000484200940700000002430613333653833652D356237612D343836352D393634612D386431633362626639616533000000042000A070000000C782D6174747269627574653200000000

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

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

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED26 (Thu Nov 12 12:10:30 CET 2009)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D5C6DF842DAEECD8
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
Tag: Attribute (0x420008), Type: Structure (0x01), Data:
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 572D4F0D433DAB10

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

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

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

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

42007B01000001A042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004AFBED2642000D0200000004000000020000000042000F01000000A042005C05000000040000000F000000004200930800000008D5C6DF842DAEED842007F050000000400000000000000042007C0100000068420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961653300000000420008010000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F64696669656456616C756531000042000F01000000A042005C05000000040000000F000000004200930800000008572D4F0D433DAB1042007F05000000040000000000000042007C0100000068420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961653300000000420008010000003042000A070000000C782D617474726962757465320000000042000B070000000E4D6F64696669656456616C7565320000

8

Client A:
Destroy (symmetric key)
In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

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

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000014000000004200790100000030420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961653300000000

Out: uuidKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED27 (Thu Nov 12 12:10:31 CET 2009)

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

```

Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
    Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004AFBED2742000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F050000000400000000000000042007C01000000304200940700000024306
13333653833652D356237612D343836352D393634612D38643163336262663961653300000000

```

9

Client A:
Get (symmetric key)
In: uuidKey

```

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A0000000042
00790100000030420094070000002430613333653833652D356237612D343836352D393634612D3864316333626266396
16533000000000

```

Out: Operation Failed, Item Not Found

```

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED27 (Thu Nov 12 12:10:31 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)
    Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x00000001 (Item Not Found)
    Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Object does not exist

42007B01000000A842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004AFBED2742000D0200000004000000010000000042000F010000005042
005C0500000004000000A0000000042007F0500000004000000010000000042007E05000000040000000100000000420

```

07D07000000154F626A65637420646F6573206E6F74206578697374000000

10

Client A:
Destroy (template)
In: uuidTemplate

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 45d8629a-9ad1-41b3-9d09-941f2a595da3

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002434356438363239612D396164312D343162332D396430392D39343166326135393564613300000000

Out: uuidTemplate

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED27 (Thu Nov 12 12:10:31 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 45d8629a-9ad1-41b3-9d09-941f2a595da3

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004AFBED2742000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002434356438363239612D396164312D343162332D396430392D39343166326135393564613300000000

11

Client A:
Get (template)
In: uuidTemplate

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 45d8629a-9ad1-41b3-9d09-941f2a595da3

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
 00000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A0000000042
 00790100000030420094070000002434356438363239612D396164312D343162332D396430392D3934316632613539356
 4613300000000

Out: Operation Failed, Item Not Found

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED27 (Thu Nov 12 12:10:31 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Failed)
 Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x00000001 (Item Not Found)
 Tag: Result Message (0x42007D), Type: Text String (0x07), Data: No Cryptographic Object found with given Unique Identifier

42007B01000000D042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
 0000000000000004200920900000008000000004AFBED2742000D0200000004000000010000000042000F010000007842
 005C05000000040000000A0000000042007F0500000004000000010000000042007E05000000040000000100000000420
 07D070000003A4E6F2043727970746F67726170686963204F626A65637420666F756E64207769746820676976656E2055
 6E69717565204964656E7469666696572000000000000

118

119 **3.1.5 Use-case: Register / Destroy Secret Data**

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

123

Time	Request/Response messages
0	Register (secret data) In: objectType='00000007' (Secret Data), attributes={ CryptographicUsageMask='00000002' } Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000007 (Secret Data)
 Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
 Mask
 Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000002 (Verify)
 Tag: Secret Data (0x420085), Type: Structure (0x01), Data:
 Tag: Secret Data Type (0x420086), Type: Enumeration (0x05), Data: 0x00000001
 Tag: Key Block (0x420040), Type: Structure (0x01), Data:
 Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000002
 Tag: Key Value (0x420045), Type: Structure (0x01), Data:
 Tag: Key Material (0x420043), Type: Octet String (0x08), Data:
 53656372657450617373776F7264

42007801000001004200770100000038420069010000002042006A0200000004000000010000000042006B0200000004
 00000000000000042000D020000000400000001000000004200F01000000B842005C05000000040000000300000000
 42007901000000A0420057050000000400000007000000004200910100000038420008010000003042000A0700000018
 43727970746F67726170686963205573616765204D61736B42000B020000000400000002000000004200850100000048
 4200860500000004000000010000000042004001000000030420042050000000400000002000000004200450100000018
 420043080000000E53656372657450617373776F72640000

Out: uuidObject

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B7924D1 (Mon Feb 15
 11:41:21 CET 2010)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 39622cc2-e5d4-4da9-
 9f10-3bdf64b0e760

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004
 000000000000000420092090000000800000004B7924D142000D020000000400000001000000004200F0100000058
 42005C0500000004000000030000000042007F05000000040000000000000042007C01000000304200940700000024
 3339363232636332D653564342D346461392D396631302D33626466363462306537363000000000

1	<p>Destroy (secret data) In: uuidObject</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

```

```

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004
000000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000001400000000
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

```

```

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004
00000000000000004200920900000008000000004B7924D142000D0200000004000000010000000042000F0100000058
42005C0500000004000000140000000042007F050000000400000000000000000042007C01000000304200940700000024
33393632326363322D653564342D346461392D396631302D33626466363462306537363000000000

```

124
125

126 **3.2 Use-case: Asynchronous Locate**

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

133

134 This use-case shows the use of two clients with the same assumptions as in the use-case described in
 135 Section 3.1.4 Since the client is unable to force the server to respond asynchronously, it is possible for a
 136 server to respond synchronously to the requests issued at times 1 and 4, in which case the expected
 137 response are the ones shown at times 2 and 5, respectively. In the case of the server not responding
 138 asynchronously to the Locate requests, the client is permitted to skip the requests illustrated at time 7 and
 139 8.
 140

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 (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage 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>Mask 42007801000001904200770100000038420069010000002042006A020000000400000001000000042006B02000000040 0000000000000042000D020000000400000001000000042000F010000014842005C050000000400000001000000042 0079010000013042005705000000040000000200000004200910100000118420008010000003042000A0700000017437 27970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200 0A070000001443727970746F67726170686963204C655E677468000000042000B0200000004000000800000000042000</p>

8010000003842000A07000000044E616D65000000042000B010000002042005507000000044B65793100000000420054
05000000040000000100000000420008010000003042000A070000001843727970746F677261706869632055736167652
04D61736B42000B0200000004000000040000000420008010000002842000A070000000C4F626A6563742047726F7570
0000000042000B070000000647726F7570310000

Out: objectType = '00000002', uuidKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED28 (Thu Nov 12 12:10:32 CET 2009)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004AFBED2842000D0200000004000000010000000042000F0100000006842
005C0500000004000000010000000042007F050000000400000000000000000000042007C010000000404200570500000004000
0000200000000420094070000002439356130653662332D386564632D346666622D613838652D6531363435339646263
636100000000

1

Client B:

Locate (symmetric key by name)

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

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

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

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

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

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

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

Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:

Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1

Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007801000000E04200770100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200070600000008000000000000000142000D0200000004000000010000000042000F010000008842005C050000000400000008000000004200790100000070420008010000002842000A070000000B4F626A6563742054797065000000000042000B05000000040000000200000000420008010000003842000A07000000044E616D650000000042000B010000002042005507000000044B6579310000000042005405000000040000000100000000

Out: asyncCorrValue1

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED28 (Thu Nov 12 12:10:32 CET 2009)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Pending)

Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 130BC369AF005A7F

42007B010000008842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000920900000008000000004AFBED2842000D0200000004000000010000000042000F010000003042005C0500000004000000080000000042007F050000000400000002000000004200060800000008130BC369AF005A7F

2

Client B:

Poll*

In: asyncCorrValue1

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll)

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

Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 130BC369AF005A7F

42007801000000704200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000002842005C050000000400000001A0000000042007901000000104200060800000008130BC369AF005A7F

Out: uuidKey1

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED28 (Thu Nov 12 12:10:32 CET 2009)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004AFBED2842000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F050000000400000000000000042007C0100000030420094070000002439356130653662332D386564632D346666622D613838652D65313634353339646263636100000000

3

Client B:
Get (symmetric key)
In: uuidKey1

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)

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

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca

420078010000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002439356130653662332D386564632D346666622D613838652D65313634353339646263636100000000

Out: objectType = '00000002', uuidKey1, symmetricKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca

Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:

Tag: Key Block (0x420040), Type: Structure (0x01), Data:

Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001

Tag: Key Value (0x420045), Type: Structure (0x01), Data:

Tag: Key Material (0x420043), Type: Octet String (0x08), Data: BEF01F82DFB4682A01C2A08413834AAB

Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)

Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2942000D020000000400000001000000004200F01000000C842005C05000000040000000A0000000042007F05000000040000000000000042007C01000000A0420057050000000400000000000000420094070000002439356130653662332D386564632D346666622D613838652D6531363435333964626363610000000042008F010000005842004001000000504200420500000004000000010000000042004501000000184200430800000010BEF01F82DFB4682A01C2A08413834AAB4200280500000004000000030000000042002A02000000040000008000000000

4

Client B:

Locate (symmetric key by group)

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

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

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

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

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

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

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

Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1

42007801000000D04200770100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2942000D020000000400000001000000004200F01000000C842005C05000000040000000A0000000042007F05000000040000000000000042007C01000000A0420057050000000400000000000000420094070000002439356130653662332D386564632D346666622D613838652D6531363435333964626363610000000042008F010000005842004001000000504200420500000004000000010000000042004501000000184200430800000010BEF01F82DFB4682A01C2A08413834AAB4200280500000004000000030000000042002A0200000004000000800000000075700000000042000B070000000647726F7570310000

Out: asyncCorrValue2

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

- Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009)
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
 - Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Pending)
 - Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 48D43C207CD1FB3A

42007B010000008842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2942000D0200000004000000010000000042000F010000003042005C0500000004000000080000000042007F05000000040000000200000000420006080000000848D43C207CD1FB3A

5

Client B:

Poll*

In: asyncCorrValue2

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

- Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll)
 - Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 48D43C207CD1FB3A

42007801000000704200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000002842005C05000000040000001A000000004200790100000010420006080000000848D43C207CD1FB3A

Out: uuidKey2

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

- Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009)
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
 - Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2942000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F050000000400000000000000042007C0100000030420094070000002439356130653662332D386564632D346666622D613838652D65313634353339646263636100000000

6

Client B:
Get (symmetric key)
In: uuidKey2

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

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002439356130653662332D386564632D346666622D613838652D65313634353339646263636100000000

Out: objectType = '00000002', uuidKey2, symmetricKey

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

BEF01F82DFB4682A01C2A08413834AAB

Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)

Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2942000D0200000004000000010000000042000F01000000C842005C05000000040000000A0000000042007F05000000040000000000000042007C01000000A042005705000000040000000000000420094070000002439356130653662332D386564632D346666622D613838652D6531363435333964626363610000000042008F01000000584200400100000050420042050000004000000010000000042004501000000184200430800000010BEF01F82DFB4682A01C2A08413834AAB4200280500000004000000030000000042002A02000000040000008000000000

7

Client B:

Locate (symmetric key by name)

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

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

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

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

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

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

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

Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:

Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1

Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007801000000E04200770100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000000420007060000000800000000000000142000D0200000004000000010000000042000F010000008842005C050000000400000008000000004200790100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B05000000040000000200000000420008010000003842000A07000000044E616D650000000042000B010000002042005507000000044B6579310000000042005405000000040000000100000000

Out: asyncCorrValue5

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12

12:10:33 CET 2009)

- Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
 - Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Pending)
 - Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 4D6BBFC35FE57FBA

42007B010000008842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2942000D0200000004000000010000000042000F010000003042005C0500000004000000080000000042007F0500000004000000020000000042000608000000084D6BBFC35FE57FBA

8

Client B:
Cancel
In: asyncCorrValue5

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

42007801000000704200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000002842005C050000000400000019000000004200790100000010420006080000000084D6BBFC35FE57FBA

Out: asyncCorrValue5, CancelResult='00000001'

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

42007B01000000A042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2942000D0200000004000000010000000042000F010000004842005C0500000004000000080000000042007F0500000004000000020000000042000608000000084D6BBFC35FE57FBA

	005C0500000004000000190000000042007F050000000400000000000000042007C010000002042000608000000084D6 BBFC35FE57FBA42001205000000040000000100000000
9	<p>Client A:</p> <p>Destroy (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: 0x00000014 (Destroy)</p> <p> Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p> Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca</p> <p>42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040 0000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000140000000042 00790100000030420094070000002439356130653662332D386564632D346666622D613838652D6531363435333964626 36361000000000</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: 0x000000004AFBED2A (Thu Nov 12 12:10:34 CET 2009)</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: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca</p> <p>42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040 000000000000004200920900000008000000004AFBED2A42000D0200000004000000010000000042000F010000005842 005C0500000004000000140000000042007F050000000400000000000000000000042007C01000000304200940700000024393 56130653662332D386564632D346666622D613838652D65313634353339646263636100000000</p>

141 * = executed until response is ready

142

143

144 **4 Key life cycle support**

145

146 **4.1 Use-case: Revoke scenario**

147 This use-case tests the revocation aspect of the key life cycle support in KMIP. A key is created and a
 148 Get Attribute for the State-attribute reveals that the key is in Pre-active state. The Activation Date is then
 149 set, which changes the state to Active. The key is then revoked with a revocation reason of Compromised
 150 and the state subsequently changed to Compromised, but this does not stop a client from being able to
 151 add, modify and delete attributes or even get the key (since we assume here that the out-of-band
 152 registration has been used to make the server aware of the fact that the client is capable of interpreting
 153 the attributes of the key and determining what it is allowed to do with the key). To clean up, the created
 154 key is finally destroyed.
 155

Time	Client
0	<p>Client A:</p> <p>Create (symmetric key)</p> <p>In: objectType = '00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', Name={ NameValue='Key1', NameType='00000001' }, CryptographicUsageMask='00000004' }</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: 0x00000001 (Create)</p> <p> Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p> Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</p> <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: Name</p> <p> Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:</p> <p> Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1</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: Cryptographic Usage Mask</p> <p> Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt)</p> <p>42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000011842005C0500000004000000010000000042007901000001004200570500000004000000020000000042009101000000E8420008010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000A070000001443727970746F67726170686963204C656E677468000000042000B02000000040000000800000000420008010000003842000A07000000044E616D650000000042000B010000002042005507000000044B65793100000000420054</p>

05000000040000000100000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000040000000400000000

Out: objectType = '00000002', uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9

42007B010000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2B42000D0200000004000000010000000042000F010000006842005C0500000004000000010000000042007F05000000040000000000000042007C010000004042005705000000040000000200000000420094070000002432316432386238612D303664662D343363302D623732662D326131363136333336164613900000000

1

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
Tag: Request Header (0x420077), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B000000004200790100000040420094070000002432316432386238612D303664662D343363302D623732662D32613136313633333616461390000000042000A07000000055374617465000000

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

```

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

42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004AFBED2B42000D0200000004000000010000000042000F0100000080842
005C05000000040000000B0000000042007F050000000400000000000000042007C01000000584200940700000024323
16432386238612D303664662D343363302D623732662D3261313631363333616461390000000042000801000000204200
0A0700000005537461746500000042000B05000000040000000100000000

```

2

```

Client A:
Activate
In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000012 (Activate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-
2a161633ada9

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000120000000042
00790100000030420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616
4613900000000

Out: uuidKey

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

```


Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000012 (Activate)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2B42000D0200000004000000010000000042000F010000005842005C0500000004000000120000000042007F050000000400000000000000042007C0100000030420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000

3

Client A:

Get attribute

In: uuidKey, attributeName={ 'State' }

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)

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

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9

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

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B000000004200790100000040420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616461390000000042000A07000000055374617465000000

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

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-

2a161633ada9

Tag: Attribute (0x420008), Type: Structure (0x01), Data:
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active)

42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000004200920900000008000000004AFBED2B42000D0200000004000000010000000042000F010000008042
005C05000000040000000B0000000042007F05000000040000000000000042007C01000000584200940700000024323
16432386238612D303664662D343363302D623732662D3261313631363333616461390000000042000801000000204200
0A0700000005537461746500000042000B05000000040000000200000000

4

Client B:

Locate (symmetric key by name)

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

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

42007801000000D04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000008842005C0500000004000000080000000042
00790100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000
0000200000000420008010000003842000A0700000004E616D65000000042000B010000002042005507000000044B65
79310000000042005405000000040000000100000000

Out: uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12
12:10:35 CET 2009)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2B42000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F050000000400000000000000042007C0100000030420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000

5

Client B:
Get (symmetric key)
In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000

Out: objectType = '00000002', uuidKey, symmetricKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
 Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
 Tag: Key Block (0x420040), Type: Structure (0x01), Data:
 Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001

Tag: Key Value (0x420045), Type: Structure (0x01), Data:
 Tag: Key Material (0x420043), Type: Octet String (0x08), Data:
 EF7833AB15F5A1EE5874BC0D9BBC4BE7

Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003
 (AES)

Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
 000000000000004200920900000008000000004AFBED2B42000D020000004000000010000000042000F01000000C842
 005C0500000004000000A000000042007F050000000400000000000000042007C01000000A04200570500000004000
 0000200000000420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164
 61390000000042008F0100000058420040010000005042004205000000040000000100000000420045010000001842004
 30800000010EF7833AB15F5A1EE5874BC0D9BBC4BE74200280500000004000000030000000042002A0200000004000000
 8000000000

6

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-
 2a161633ada9
 Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:
 Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000002 (Key
 Compromise)
 Tag: Compromise Occurrence Date (0x420021), Type: Date-Time (0x09), Data:
 0x0000000000000006 (Thu Jan 01 01:00:06 CET 1970)

42007801000000B84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
 000000000000042000D020000004000000010000000042000F010000007042005C0500000004000000130000000042
 00790100000058420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616
 461390000000042008101000000104200820500000004000000020000000042002109000000080000000000000006

Out: uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12
 12:10:35 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004AFBED2B42000D0200000004000000010000000042000F010000005842005C0500000004000000130000000042007F050000000400000000000000042007C0100000030420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000

7

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B0000000042007901000000040420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616461390000000042000A07000000055374617465000000

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

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2C (Thu Nov 12 12:10:36 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
 Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Compromised)

```
42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2C42000D0200000004000000010000000042000F0100000008042005C05000000040000000B0000000042007F050000000400000000000000042007C0100000058420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000420008010000002042000A0700000005537461746500000042000B05000000040000000400000000
```

8

Client A:
Get attribute list
In: uuidKey

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

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000C000000004200790100000030420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000

Out: uuidKey, attributes = { * }

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

Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Unique Identifier
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Last Change Date

42007B010000022042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004AFBED2C42000D0200000004000000010000000042000F01000001C842
005C05000000040000000C0000000042007F050000000400000000000000042007C01000001A04200940700000024323
16432386238612D303664662D343363302D623732662D3261313631363333616461390000000042000A07000000144372
7970746F67726170686963204C656E677468000000042000A070000001743727970746F6772617068696320416C676F7
26974686D0042000A0700000005537461746500000042000A070000001A436F6D70726F6D697365204F6363757272656E
636520446174650000000000042000A07000000F436F6D70726F6D69736520446174650042000A07000000064469676
57374000042000A070000000C496E697469616C20446174650000000042000A070000000F41637469766174696F6E2044
6174650042000A07000000115265766F636174696F6E20526561736F6E000000000000042000A0700000011556E69717
565204964656E746966696572000000000000042000A0700000044E616D65000000042000A07000000184372797074
6F67726170686963205573616765204D61736B42000A07000000B4F626A656374205479706500000000042000A07000
000104C617374204368616E67652044617465

9

Client A:

Get attributes

In: uuidKey, attributeName = { 'State' }

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
Tag: Request Header (0x420077), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-
2a161633ada9
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B0000000042
00790100000040420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616
461390000000042000A07000000055374617465000000

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

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004AFBED2C (Thu Nov 12
12:10:36 CET 2009)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)

```

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
    Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
    Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Compromised)

42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004AFBED2C42000D0200000004000000010000000042000F010000008042
005C05000000040000000B0000000042007F05000000040000000000000042007C01000000584200940700000024323
16432386238612D303664662D343363302D623732662D3261313631363333616461390000000042000801000000204200
0A0700000005537461746500000042000B050000000400000000400000000

```

10

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

```

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 9D407FFB45C95672
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value1
    Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
      Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D62107C3158409D8
      Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
        Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value2

42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000020000000042000F010000008842005C05000000040000000D0000000042
009308000000089D407FFB45C956724200790100000060420094070000002432316432386238612D303664662D3433633
02D623732662D32613136313633336164613900000000420008010000002842000A070000000C782D6174747269627574
65310000000042000B070000000656616C756531000042000F010000008842005C05000000040000000D0000000042009
30800000008D62107C3158409D84200790100000060420094070000002432316432386238612D303664662D343363302D
623732662D32613136313633336164613900000000420008010000002842000A070000000C782D6174747269627574653
20000000042000B070000000656616C7565320000

```


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

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2C (Thu Nov 12 12:10:36 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 9D407FFB45C95672
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value1
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D62107C3158409D8
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value2

42007B010000019042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004AFBED2C42000D0200000004000000020000000042000F010000009842
005C05000000040000000D0000000042009308000000089D407FFB45C9567242007F050000000400000000000000420
07C01000000060420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164
613900000000420008010000002842000A070000000C782D617474726962757465310000000042000B070000000656616
C756531000042000F010000009842005C05000000040000000D000000004200930800000008D62107C3158409D842007F
05000000040000000000000042007C0100000060420094070000002432316432386238612D303664662D343363302D6
23732662D32613136313633336164613900000000420008010000002842000A070000000C782D61747472696275746532
0000000042000B070000000656616C7565320000

11	<p>Client A: Modify attribute [batch] In: uuidKey, attribute={ x-attribute1='ModifiedValue1' } In: uuidKey, attribute={ x-attribute2='ModifiedValue2' }</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)</p>
----	---

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 47FB42CCECA3F6EC

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

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9

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

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

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 08019A230A05E9E1

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

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9

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

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

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

```
42007801000001704200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D02000000040000000020000000042000F010000009042005C05000000040000000E0000000042
0093080000000847FB42CCECA3F6EC4200790100000068420094070000002432316432386238612D303664662D3433633
02D623732662D32613136313633336164613900000000420008010000003042000A070000000C782D6174747269627574
65310000000042000B070000000E4D6F64696669656456616C756531000042000F010000009042005C050000000400000
00E0000000042009308000000808019A230A05E9E14200790100000068420094070000002432316432386238612D3036
64662D343363302D623732662D32613136313633336164613900000000420008010000003042000A070000000C782D617
474726962757465320000000042000B070000000E4D6F64696669656456616C7565320000
```

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

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

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2D (Thu Nov 12 12:10:37 CET 2009)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 47FB42CCECA3F6EC

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9

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

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

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 08019A230A05E9E1
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2

42007B01000001A042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED2D42000D0200000004000000020000000042000F01000000A042005C05000000040000000E00000000420093080000000847FB42CCECA3F6EC42007F05000000040000000000000042007C010000000684200940700000002432316432386238612D303664662D343363302D623732662D3261313631363333616461390000000042008010000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F64696669656456616C756531000042000F01000000A042005C05000000040000000E00000000420093080000000808019A230A05E9E142007F05000000040000000000000042007C010000000684200940700000002432316432386238612D303664662D343363302D623732662D3261313631363333616461390000000042008010000003042000A070000000C782D617474726962757465320000000042000B070000000E4D6F64696669656456616C7565320000

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3E2C080FA8806057
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 9D55988D43D23B82
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2

42007801000001304200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000020000000042000F010000007042005C05000000040000000F0000000042009308000000083E2C080FA880605742007901000000484200940700000002432316432386238612D303664662D343363302D623732662D3261313631363333616461390000000042000A070000000C782D617474726962757465310000000042000B070000000E4D6F64696669656456616C7565320000000042009308000000089D55988D43D23B8242007901000000484200940700000002432316432386238612D303664662D343363302D623732662D3261313631363333616461390000000042000A070000000C782D6174747269627574653200000000

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

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

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

42007B01000001A042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004AFBED2D42000D0200000004000000020000000042000F01000000A042005C050000000400000000F0000000042009308000000083E2C080FA880605742007F0500000004000000000000000042007C010000000684200940700000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000420008010000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F64696669656456616C756531000042000F01000000A042005C050000000400000000F0000000042009308000000089D55988D43D23B8242007F05000000040000000000000042007C010000000684200940700000002432316432386238612D303664662D343363302D623732662D32613136313633336164662D343363302D623732662D3261313631363333616461390000000042000B070000000E4D6F64696669656456616C7565320000

13 Client A:
Get (symmetric key)
In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000

Out: objectType = '00000002', uuidKey, symmetricKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2D (Thu Nov 12 12:10:37 CET 2009)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
 Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
 Tag: Key Block (0x420040), Type: Structure (0x01), Data:
 Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
 Tag: Key Value (0x420045), Type: Structure (0x01), Data:
 Tag: Key Material (0x420043), Type: Octet String (0x08), Data: EF7833AB15F5A1EE5874BC0D9BBC4BE7
 Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
 Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F01000000C842005C05000000040000000A0000000042007F050000000400000000000000042007C01000000A042005705000000040000000000000420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616461390000000042008F010000005842004001000000504200420500000004000000010000000042004501000000184200430800000010EF7833AB15F5A1EE5874BC0D9BBC4BE7420028050000000400000030000000042002A02000000040000008000000000

14	<p>Client A: Destroy (symmetric key) 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)</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: 21d28b8a-06df-43c0-b72f-2a161633ada9

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000140000000042
007901000000304200940700000002432316432386238612D303664662D343363302D623732662D3261313631363333616
4613900000000

```

Out: uuidKey

```

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000004200920900000008000000004AFBED2E42000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F0500000004000000000000000042007C010000003042009407000000024323
16432386238612D303664662D343363302D623732662D32613136313633336164613900000000

```

156

157

158 **5 Auditing and reporting**

159

160 **5.1 Use-case: Get usage allocation scenario**

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

168

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

0

Client A:

Create (symmetric key)

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)

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

Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:

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

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

Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)

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

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

Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)

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

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

Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:

Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1

Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

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

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

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

42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B020000000400
000000000000042000D0200000004000000010000000042000F010000011842005C050000000400000001000000004200
7901000001004200570500000004000000020000000042009101000000E84200080100000003042000A0700000017437279
70746F6772617068696320416C676F726974686D0042000B050000000400000003000000004200080100000003042000A07
0000001443727970746F67726170686963204C656E677468000000042000B020000000400000008000000004200080100
00003842000A07000000044E616D650000000042000B010000002042005507000000044B65793100000000420054050000
000400000001000000004200080100000003042000A070000001843727970746F67726170686963205573616765204D6173
6B42000B02000000040000000400000000

Out: objectType = '00000002', uuidKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05A (Thu Mar 11 13:21:46 CET 2010)

Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29bald

 42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400
 000000000000004200920900000008000000004B98E05A42000D0200000004000000010000000042000F01000000684200
 5C0500000004000000010000000042007F050000000400000000000000042007C01000000404200570500000004000000
 0200000000420094070000002465363936656264302D386562612D343036652D626532312D643930353965323962613164
 00000000

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

 Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D7FE2477E364AE1A
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29bald
 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 (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 9696012991BC8A59
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29bald
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date
 Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B98E2B3 (Thu Mar 11 13:31:47 CET 2010)

 42007801000001684200770100000038420069010000002042006A0200000004000000010000000042006B020000000400
 0000000000000042000D0200000004000000020000000042000F010000008842005C05000000040000000D000000004200
 930800000008D7FE2477E364AE1A4200790100000060420094070000002465363936656264302D386562612D343036652D
 626532312D64393035396532396261316400000000420008010000002842000A070000000F41637469766174696F6E2044
 6174650042000B090000000800000000000000242000F010000009042005C05000000040000000D000000004200930800
 0000089696012991BC8A594200790100000068420094070000002465363936656264302D386562612D343036652D626532
 312D64393035396532396261316400000000420008010000003042000A070000001150726F746563742053746F70204461

7465000000000000042000B0900000008000000004B98E2B3

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

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05B (Thu Mar 11 13:21:47 CET 2010)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D7FE2477E364AE1A
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29bald
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 (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 9696012991BC8A59
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29bald
Tag: Attribute (0x420008), Type: Structure (0x01), Data:
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date
Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B98E2B3 (Thu Mar 11 13:31:47 CET 2010)

42007B010000019842007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400
000000000000004200920900000008000000004B98E05B42000D0200000004000000020000000042000F01000000984200
5C05000000040000000D000000004200930800000008D7FE2477E364AE1A42007F050000000400000000000000042007C
0100000060420094070000002465363936656264302D386562612D343036652D626532312D643930353965323962613164
00000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B09000000080000000000
00000242000F01000000A042005C05000000040000000D0000000042009308000000089696012991BC8A5942007F050000
000400000000000000042007C0100000068420094070000002465363936656264302D386562612D343036652D62653231
2D64393035396532396261316400000000420008010000003042000A070000001150726F746563742053746F7020446174
65000000000000042000B0900000008000000004B98E2B3

2 Client A:
Add Attribute
In: uuidKey, attribute={ UsageLimits={ UsageLimitsTotal='1000', UsageLimitsUnit='1' } }

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-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 (0x420097), Type: Long Integer (0x03), Data: 0x000000000000003E8
 (1000)
 Tag: Usage Limits Unit (0x420098), Type: Enumeration (0x05), Data: 0x00000001 (Byte)

42007801000000D84200770100000038420069010000002042006A0200000004000000010000000042006B020000000400
 000000000000042000D0200000004000000010000000042000F010000009042005C05000000040000000D000000004200
 790100000078420094070000002465363936656264302D386562612D343036652D626532312D6439303539653239626131
 6400000000420008010000004042000A070000000C5573616765204C696D6974730000000042000B010000002042009703
 00000008000000000000003E842009805000000040000000100000000

Out: uuidKey, attribute={ UsageLimits={ UsageLimitsTotal= '1000', UsageLimitsCount='1000', UsageLimitsUnit='1' } }

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05C (Thu Mar 11 13:21:48 CET 2010)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-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 (0x420097), Type: Long Integer (0x03), Data: 0x000000000000003E8
 (1000)
 Tag: Usage Limits Count (0x420096), Type: Long Integer (0x03), Data: 0x000000000000003E8
 (1000)
 Tag: Usage Limits Unit (0x420098), Type: Enumeration (0x05), Data: 0x00000001 (Byte)

42007B010000010842007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400
 00000000000004200920900000008000000004B98E05C42000D0200000004000000010000000042000F01000000B04200
 5C05000000040000000D0000000042007F05000000040000000000000042007C01000000884200940700000024653639
 36656264302D386562612D343036652D626532312D64393035396532396261316400000000420008010000005042000A07
 0000000C5573616765204C696D6974730000000042000B01000000304200970300000008000000000000003E84200960300

000008000000000000000003E842009805000000040000000100000000

3

Client B:

Locate (symmetric key by name)

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

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

42007801000000D04200770100000038420069010000002042006A0200000004000000010000000042006B020000000400
0000000000000042000D0200000004000000010000000042000F010000008842005C050000000400000008000000004200
790100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000
0200000000420008010000003842000A07000000044E616D65000000042000B010000002042005507000000044B657931
0000000042005405000000040000000100000000

Out: uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05C (Thu Mar 11
13:21:48 CET 2010)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-
d9059e29bald

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400
000000000000004200920900000008000000004B98E05C42000D0200000004000000010000000042000F01000000584200
5C0500000004000000080000000042007F050000000400000000000000042007C01000000304200940700000024653639

36656264302D386562612D343036652D626532312D64393035396532396261316400000000

4

Client B:

Get (symmetric key)

In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)

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

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

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002465363936656264302D386562612D343036652D626532312D64393035396532396261316400000000

Out: objectType = '00000002', uuidKey, symmetricKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05C (Thu Mar 11 13:21:48 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

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

Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:

Tag: Key Block (0x420040), Type: Structure (0x01), Data:

Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001

Tag: Key Value (0x420045), Type: Structure (0x01), Data:

Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 674B32B1A3266DF1253B0F2C4440B0B0

Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)

Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B98E05C42000D0200000004000000010000000042000F01000000C84200

5C05000000040000000A0000000042007F050000000400000000000000042007C01000000A04200570500000004000000
02000000004200940700000002465363936656264302D386562612D343036652D626532312D643930353965323962613164
0000000042008F01000000584200400100000050420042050000000400000001000000042004501000000184200430800
000010674B32B1A3266DF1253B0F2C4440B0B04200280500000004000000030000000042002A02000000040000000800000
0000

5 Client B:
Check
Get usage allocation
In (header): BatchOrderOption='true'
In: uuidKey, UsageLimitsCount='500'
In: uuidKey, UsageLimitsCount='500'

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000009 (Check)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 19D4F3DC9635307A
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29bald
 Tag: Usage Limits Count (0x420096), Type: Long Integer (0x03), Data: 0x00000000000001F4 (500)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 20C8DFFD55BDEEE8
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29bald
 Tag: Usage Limits Count (0x420096), Type: Long Integer (0x03), Data: 0x00000000000001F4 (500)

42007801000001204200770100000038420069010000002042006A0200000004000000010000000042006B020000000400
0000000000000042000D0200000004000000020000000042000F010000006842005C050000000400000009000000004200
93080000000819D4F3DC9635307A4200790100000040420094070000002465363936656264302D386562612D343036652D
626532312D643930353965323962613164000000004200960300000080000000000001F442000F010000006842005C05
00000004000000110000000042009308000000820C8DFFD55BDEEE8420079010000004042009407000000246536393665
6264302D386562612D343036652D626532312D6439303539653239626131640000000042009603000000800000000000
01F4

Out: uuidKey
Out: uuidKey

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

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05D (Thu Mar 11 13:21:49 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000009 (Check)

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

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

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

42007B010000013042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400
000000000000004200920900000008000000004B98E05D42000D0200000004000000020000000042000F01000000684200
5C05000000040000000900000000420093080000000819D4F3DC9635307A42007F050000000400000000000000042007C
01000000304200940700000002465363936656264302D386562612D343036652D626532312D643930353965323962613164
0000000042000F010000006842005C05000000040000001100000000420093080000000820C8DFFD55BDEEE842007F0500
000004000000000000000042007C01000000304200940700000002465363936656264302D386562612D343036652D626532
312D64393035396532396261316400000000

6

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

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

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

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

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

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B020000000400
0000000000000042000D0200000004000000010000000042000F010000005842005C050000000400000011000000004200
7901000000404200940700000002465363936656264302D386562612D343036652D626532312D6439303539653239626131
6400000000420096030000000800000000000001F4

Out: uuidKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05D (Thu Mar 11 13:21:49 CET 2010)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29bald

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B98E05D42000D0200000004000000010000000042000F010000005842005C0500000004000000110000000042007F050000000400000000000000042007C0100000030420094070000002465363936656264302D386562612D343036652D626532312D64393035396532396261316400000000

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

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

42007801000000D04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000008842005C050000000400000008000000004200790100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B05000000040000000200000000420008010000003842000A07000000044E616D650000000042000B010000002042005507000000044B657931000000042005405000000040000000100000000

Out: uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05D (Thu Mar 11 13:21:49 CET 2010)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29bald

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B98E05D42000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F05000000040000000000000042007C0100000030420094070000002465363936656264302D386562612D343036652D626532312D64393035396532396261316400000000

8

Client C:
Get (symmetric key)
In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29bald

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002465363936656264302D386562612D343036652D626532312D64393035396532396261316400000000

Out: objectType = '00000002', uuidKey, symmetricKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05D (Thu Mar 11 13:21:49 CET 2010)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

- Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
- Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29bald
- Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
 - Tag: Key Block (0x420040), Type: Structure (0x01), Data:
 - Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
 - Tag: Key Value (0x420045), Type: Structure (0x01), Data:
 - Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 674B32B1A3266DF1253B0F2C4440B0B0
 - Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
 - Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B98E05D42000D0200000004000000010000000042000F01000000C842005C05000000040000000A0000000042007F050000000400000000000000042007C01000000A0420057050000000400000000200000000420094070000002465363936656264302D386562612D343036652D626532312D643930353965323962613164000000042008F01000000584200400100000050420042050000000400000001000000004200450100000018420043080000010674B32B1A3266DF1253B0F2C4440B0B04200280500000004000000030000000042002A020000000400000080000000

9

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

- Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)
 - Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-d9059e29bald
 - Tag: Usage Limits Count (0x420096), Type: Long Integer (0x03), Data: 0x00000000000001F4 (500)

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000005842005C050000000400000001100000000420005C050000000400000002465363936656264302D386562612D343036652D626532312D64393035396532396261316400000000420096030000000800000000000001F4

Out: Operation Failed, Permission Denied

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

- Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05D (Thu Mar 11

13:21:49 CET 2010)

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

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

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

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)

Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x0000000C (Permission Denied)

Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Unable to allocate requested amount

42007B01000000B842007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B98E05D42000D0200000004000000010000000042000F010000006042005C0500000004000000110000000042007F0500000004000000010000000042007E05000000040000000C0000000042007D0700000023556E61626C6520746F20616C6C6F636174652072657175657374656420616D6F756E740000000000

10

Client A:

Revoke (symmetric key as cessation of operation) and Destroy (symmetric key)

In (header): batchOrderOption='TRUE'

In: uuidKey, revocationReasonCode='6'

In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)

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

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

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

Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:

Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000006 (Cessation of Operation)

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

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

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

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

42007801000001284200770100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000420010060000000800000000000000142000D0200000004000000020000000042000F010000007042005C050000000400000013000000004200930800000008727A212BC674B4EA4200790100000048420094070000002465363936656264302D386562612D343036652D626532312D643930353965323962613164000000004200810100000010420082050000004000000060000000042000F010000005842005C05000000040000001400000004200930800000081D0EBF826109B0A54200790100000030420094070000002465363936656264302D386562612D343036652D626532312D64393035396532396261316400000000

Out: uuidKey

Out: uuidKey

```

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B98E05F (Thu Mar 11 13:21:51 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 727A212BC674B4EA
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: e696ebd0-8eba-406e-be21-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
0000000000004200920900000008000000004B98E05F42000D0200000004000000020000000042000F01000000684200
5C050000000400000013000000004200930800000008727A212BC674B4EA42007F050000000400000000000000042007C
01000000304200940700000002465363936656264302D386562612D343036652D626532312D643930353965323962613164
0000000042000F010000006842005C0500000004000000140000000042009308000000081D0EBF826109B0A542007F0500
000004000000000000000042007C01000000304200940700000002465363936656264302D386562612D343036652D626532
312D64393035396532396261316400000000

```

169
170
171
172

6 Key Interchange, Key Exchange

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

173
174
175
176
177
178

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

Time	Request/Response messages
0	Register (symmetric key) In: objectType = '00000002', attributes={ CryptographicUsageMask='00000004' }, foreignSymmetricKey Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

- Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
- Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

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

- Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
- Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 - Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
 - Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 - Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
 - Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt)
 - Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
 - Tag: Key Block (0x420040), Type: Structure (0x01), Data:
 - Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
 - Tag: Key Value (0x420045), Type: Structure (0x01), Data:
 - Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 0123456789ABCDEF0123456789ABCDEF
 - Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
 - Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

42007801000001104200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000000C842005C0500000004000000030000000042007901000000B0420057050000000400000002000000004200910100000038420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000040000000042008F0100000058420040010000005042004205000000040000000100000000420045010000001842004308000000100123456789ABCDEF0123456789ABCDEF4200280500000004000000030000000042002A02000000040000000800000000

Out: uuidKey

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

- Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED32 (Thu Nov 12 12:10:42 CET 2009)
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
 - Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 - Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED3242000D0200000004000000010000000042000F010000005842005C0500000004000000030000000042007F050000000400000000000000042007C0100000030420094070000002436653161356138332D383131332D343236302D623430642D39363666323331623931623700000000

1	<p>Add attribute</p> <p>In: uuidKey, attribute={ x-provider='unknown' }</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: 0x0000000D (Add Attribute)</p> <p> Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p> Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7</p> <p> Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p> Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-provider</p> <p> Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: unknown</p> <p>42007801000000C04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000007842005C05000000040000000D000000004200790100000060420094070000002436653161356138332D383131332D343236302D623430642D39363666323331623931623700000000420008010000002842000A07000000A782D70726F76696465720000000000042000B0700000007756E6B6E6F776E00</p> <p>Out: uuidKey, attribute={ x-provider='unknown' }</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: 0x00000004AFBED32 (Thu Nov 12 12:10:42 CET 2009)</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: 0x0000000D (Add Attribute)</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: 6e1a5a83-8113-4260-b40d-966f231b91b7</p> <p> Tag: Attribute (0x420008), Type: Structure (0x01), Data:</p> <p> Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-provider</p> <p> Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: unknown</p> <p>42007B01000000E042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED3242000D0200000004000000010000000042000F010000008842005C05000000040000000D0000000042007F0500000004000000000000000042007C0100000060420094070000002436653161356138332D383131332D343236302D623430642D39363666323331623931623700000000420008010000002842000A07000000A782D70726F76696465720000000000042000B0700000007756E6B6E6F776E00</p>
2	<p>Modify attribute</p>

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
Tag: Request Header (0x420077), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7
Tag: Attribute (0x420008), Type: Structure (0x01), Data:
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-provider
Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: third party

42007801000000C84200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000008042005C05000000040000000E000000004200790100000068420094070000002436653161356138332D383131332D343236302D623430642D39363666323331623931623700000000420008010000003042000A070000000A782D70726F76696465720000000000042000B070000000B74686972642070617274790000000000

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

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004AFBEB32 (Thu Nov 12 12:10:42 CET 2009)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7
Tag: Attribute (0x420008), Type: Structure (0x01), Data:
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-provider
Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: third party

42007B01000000E842007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004AFBEB324200D0200000004000000010000000042000F010000009042005C05000000040000000E0000000042007F05000000040000000000000042007C0100000068420094070000002436653161356138332D383131332D343236302D623430642D39363666323331623931623700000000420008010000003042000A070000000A782D70726F766964657200000000000042000B070000000B74686972642070617274790000000000

3

Destroy (symmetric key)

In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
Tag: Request Header (0x420077), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000014000000004200790100000030420094070000002436653161356138332D383131332D343236302D623430642D39363666323331623931623700000000

Out: uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED32 (Thu Nov 12 12:10:42 CET 2009)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004AFBED3242000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F050000000400000000000000042007C0100000030420094070000002436653161356138332D383131332D343236302D623430642D39363666323331623931623700000000

179
180
181

7 Vendor Extensions

182
183
184

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

185 **7.1 Use-case: Unrecognized Message Extension with Criticality Indicator**
 186 **false**

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

190

Time	Client A
0	<p>Create (symmetric key)</p> <p>In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C' }, MessageExtension={ VendorIdentification='Acme', CriticalityIndicator='false', VendorExtension={ tag='0x540001', type='text string', value='na' } }</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: 0x00000001 (Create)</p> <p>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p>Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</p> <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 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 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 Usage Mask</p> <p>Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)</p> <p>Tag: Message Extension (0x420051), Type: Structure (0x01), Data:</p> <p>Tag: Criticality Indicator (0x420026), Type: Boolean (0x06), Data: FALSE</p> <p>Tag: Vendor Identification (0x42009D), Type: Text String (0x07), Data: Acme</p> <p>Tag: Vendor Extension (0x42009C), Type: Structure (0x01), Data:</p> <p>Tag: Unknown tag (0x014242), Type: Text String (0x07), Data: na</p> <p>42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D020000000400000001000000042000F010000011842005C0500000004000000010000000042007901000000C0420057050000000400000002000000042009101000000A8420008010000003042000A070000001443727970746F67726170686963204C656E677468000000042000B02000000040000008000000000420008010000003042000A0700000001743727970746F6772617068696320416C676F726974686D0042000B050000000400000003000000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000040000000C000000000420051010000003842002606000000800000000000000042009D070000000441636D650000000042009C01000001001424207000000026E61000000000000</p>

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

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000042009209000000800000004B73BF1C42000D0200000004000000010000000042000F010000006842005C0500000004000000010000000042007F050000000400000000000000042007C0100000040420057050000000400000020000000420094070000002430353265666637332D623335652D343730322D396462392D33376331326630313531643300000000

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

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000014000000004200790100000030420094070000002430353265666637332D623335652D343730322D396462392D33376331326630313531643300000000

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004B73BF1C42000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F050000000400000000000000042007C01000000304200940700000024303
53265666637332D623335652D343730322D396462392D33376331326630313531643300000000

```

191

192

193 **7.2 Use-case: Unrecognized Message Extension with Criticality Indicator**
194 **true**

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

198

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>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</p>

Mask

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

Tag: Message Extension (0x420051), Type: Structure (0x01), Data:

Tag: Criticality Indicator (0x420026), Type: Boolean (0x06), Data: TRUE

Tag: Vendor Identification (0x42009D), Type: Text String (0x07), Data: Acme

Tag: Vendor Extension (0x42009C), Type: Structure (0x01), Data:

Tag: Unknown tag (0x014242), Type: Text String (0x07), Data: na

```
42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000D02000000040000000010000000042000F010000011842005C0500000004000000010000000042
007901000000C042005705000000040000000020000000042009101000000A8420008010000003042000A0700000014437
27970746F67726170686963204C656E6774680000000042000B0200000004000000800000000042000801000000304200
0A070000001743727970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000
8010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000
0C000000004200510100000038420026060000000800000000000000142009D070000000441636D650000000042009C0
10000001001424207000000026E61000000000000
```

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

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004B73BF1D42000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F0500000004000000010000000042007E0500000004000000800000000420
07D0700000029437269746963616C204D65737361676520457874656E73696F6E206E6F74207265636F676E697A656400
000000000000
```

199

200

201

202 8 Asymmetric keys

203

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

205 8.1 Use-case: Create a Key Pair

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

Time	Client A
0	<p>Create Key Pair</p> <p>In: commonAttributes={ CryptographicAlgorithm='RSA', CryptographicLength='1024' }, privateKeyAttributes={ Name={ NameValue='PrivateKey1', NameType='00000001' }, CryptographicUsageMask='00000001' }, publicKeyAttributes={ NameValue='PublicKey1', NameType='00000001' }, CryptographicUsageMask='00000002' }</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: 0x00000002 (Create Key Pair)</p> <p> Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p> Tag: Common Template-Attribute (0x42001F), 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: 0x00000004 (RSA)</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: 0x00000400 (1024)</p> <p> Tag: Private Key Template-Attribute (0x420065), 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 (0x420055), Type: Text String (0x07), Data: PrivateKey1</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: Cryptographic Usage Mask</p> <p> Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000001 (Sign)</p> <p> Tag: Public Key Template-Attribute (0x42006E), 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 (0x420055), Type: Text String (0x07), Data: PublicKey1</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: Cryptographic Usage Mask</p> <p> Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000002 (Verify)</p> <p>42007801000001E84200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F01000001A042005C0500000004000000020000000420079010000018842001F0100000070420008010000003042000A070000001743727970746F6772617068696320416C676</p>

F726974686D0042000B05000000040000000400000000420008010000003042000A070000001443727970746F67726170686963204C656E6774680000000042000B020000000400000040000000004200650100000080420008010000004042000A07000000044E616D650000000042000B0100000028420055070000000B507269766174654B65793100000000042005405000000040000000100000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000010000000042006E0100000080420008010000004042000A07000000044E616D650000000042000B010000002842005507000000A5075626C69634B65793100000000004200540500000004000000010000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B020000040000000200000000

Out: uuidPrivateKey, uuidPublicKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13A (Thu Feb 11 09:35:06 CET 2010)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000002 (Create Key Pair)
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-6dc2115cc042
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-879bab490259

42007B01000000E042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000000400000000000004200920900000008000000004B73C13A42000D0200000004000000010000000042000F010000008842005C0500000004000000020000000042007F05000000040000000000000042007C0100000060420094070000002438393566373263322D623230612D343964382D393530342D36646332313135636330343200000000420094070000002461323432666361342D656266302D343339382D616336352D38373962616234393032353900000000

1	<p>Locate (Public Key)</p> <p>In: attributes={ objectType='PublicKey', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } }</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: 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:</p>
---	---

Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000103 (Private Key Link)

Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-879bab490259

42007801000000F04200770100000038420069010000002042006A0200000004000000010000000042006B020000000400000000000042000D0200000004000000010000000042000F01000000A842005C050000000400000008000000004200790100000090420008010000002842000A070000000B4F626A656374205479706500000000042000B050000000400000000300000000420008010000005842000A07000000044C696E6B0000000042000B010000004042004B0500000004000001030000000042004C070000002461323432666361342D656266302D343339382D616336352D38373962616234393032353900000000

Out: uuidPublicKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13B (Thu Feb 11 09:35:07 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-6dc2115cc042

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000920900000008000000004B73C13B42000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F050000000400000000000000042007C0100000030420094070000002438393566373263322D623230612D343964382D393530342D36646332313135636330343200000000

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

42007801000000F04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F01000000A842005C050000000400000008000000004200790100000090420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000000420008010000005842000A07000000044C696E6B0000000042000B010000004042004B0500000004000001020000000042004C070000002438393566373263322D623230612D343964382D393530342D36646332313135636330343200000000

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B73C13B42000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F05000000040000000000000042007C0100000030420094070000002461323432666361342D656266302D343339382D616336352D38373962616234393032353900000000

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:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-879bab490259

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B73C13B42000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F050000000400000000000000042007C0100000030420094070000002461323432666361342D656266302D343339382D616336352D38373962616234393032353900000000

4

Destroy
In: uuidPublicKey

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

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002438393566373263322D623230612D343964382D393530342D36646332313135636330343200000000

Out: uuidPublicKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13B (Thu Feb 11


```

09:35:07 CET 2010)
  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-
6dc2115cc042

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004B73C13B42000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F050000000400000000000000042007C01000000304200940700000024383
93566373263322D623230612D343964382D393530342D36646332313135636330343200000000

```

209

210 **8.2 Use-case: Register Both Halves of a Key Pair**

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

213

Time	Client A
0	<p>Register (Private Key) In: objectType='00000004', attributes={ CryptographicUsageMask='00000001' }, foreignPrivateKey</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: 0x00000003 (Register) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000004 (Private Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000001 (Sign) Tag: Private Key (0x420064), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000004 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 30820276020100300D06092A864886F70D0101010500048202603082025C02010002818100930451C9ECD94F5BB9DA17D D09381BD23BE43ECA8C7539F301FC8A8CD5D274C3E7699DBDC711C97A7AA91E2C50A82BD0B1034F0DF493DEC16362427 E58ACCE7F6CE0F9BCC617BBD8C90D0094A2703BA0D09EB19D1005F2FB265526AAC75AF32F8BC782CDED2A57F811E03EAF 67A944DE5E78413DCA8F232D074E6DCEA4CEC9F02030100010281800B6A7D736199EA48A420E4537CA0C7C046784DCBEA A63BAEBC0BC132787449CDE8D7CAD0C0C863C0FEFB06C3062BEFC50033ECF87B4E33A9BE7BCBC8F1511AE215E80DEB5D8 AF2BD31319D7821196640935A0CD67C94599579F2100D65E038831FDAFB0DBE2BBDAC00A696E67E756350E1C99ACE11A3 6DABAC3ED3E730960059024100DDF672FBCC5BDA3D73AFFC4E791E0C03390224405D69CCAABC749FAA0DCD4C2583C71DD E8941A7B9AA030F52EF1451466C074D4D338FE677892ACD9E10FD35BD024100A98FBC3ED6B4C6F860F97165AC2F7BB6F2</p>

E2CB192A9ABD49795BE5BCF37D8EE69A6E169C24E5C32E4E7FA33265461407F952BA49E204818A2F785F113F922B8B0240253F9470390D39049303777DDBC9750E9D64849CE0903EAE704DC9F589B7680DEB9D609FD5BCD4DECD6F120542E5CFF5D76F2A43C8615FB5B3A9213463797AA9024100A1DDDF023C0CD94C019BB26D09B9E3CA8FA971CB16AA58B9BAF79D6081A1DBBA452BA53653E2804BA98FF69E8BB1B3A161EA225EA501463216A8DAB9B88A75E5F02406178646E112CF79D921A8A843F17F6E7FF974F688122365BF6690CDFC996E1890952EB3820DD1890EC1C8619E87A2BD38F9D03B37FAC742EFB748C7885942C39

Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000004 (RSA)

Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000400 (1024)

42007801000003804200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000033842005C05000000040000000300000000420079010000032042005705000000040000000400000004200910100000038420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000010000000042006401000002C842004001000002C042004205000000040000000400000004200450100000288420043080000027A30820276020100300D06092A864886F70D0101010500048202603082025C02010002818100930451C9ECD94F5BB9DA17DD09381BD23BE43ECA8C7539F301FC8A8CD5D5274C3E7699DBDC711C97A7AA91E2C50A82BD0B1034F0DF493DEC16362427E58ACCE7F6CE0F9BCC617BBD8C90D0094A2703BA0D09EB19D1005F2FB265526AAC75AF32F8BC782CED2A57F811E03EAF67A944DE5E78413DCA8F232D074E6DCEA4CEC9F02030100010281800B6A7D736199EA48A420E4537CA0C7C046784DCBEAA63BAEBC0BC132787449CDE8D7CAD0C0C863C0FEFB06C3062BEFC50033ECF87B4E33A9BE7BCBC8F1511AE215E80DEB5D8AF2BD31319D7821196640935A0CD67C94599579F2100D65E038831FDAFB0DBE2BBDAC00A696E67E756350E1C99ACE11A36DABAC3ED3E730960059024100DDF672FBCC5BDA3D73AFFC4E791E0C03390224405D69CCAABC749FAA0DCD4C2583C71DDE8941A7B9AA030F52EF1451466C074D4D338FE677892ACD9E10FD35BD024100A98FBC3ED6B4C6F860F97165AC2F7BB6F2E2CB192A9ABD49795BE5B CF37D8EE69A6E169C24E5C32E4E7FA33265461407F952BA49E204818A2F785F113F922B8B0240253F9470390D39049303777DDBC9750E9D64849CE0903EAE704DC9F589B7680DEB9D609FD5BCD4DECD6F120542E5CFF5D76F2A43C8615FB5B3A9213463797AA9024100A1DDDF023C0CD94C019BB26D09B9E3CA8FA971CB16AA58B9BAF79D6081A1DBBA452BA53653E2804BA98FF69E8BB1B3A161EA225EA501463216A8DAB9B88A75E5F02406178646E112CF79D921A8A843F17F6E7FF974F688122365BF6690CDFC996E1890952EB3820DD1890EC1C8619E87A2BD38F9D03B37FAC742EFB748C7885942C390000000000042002A02000000040000040000000000

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: 0x00000004B73C4A1 (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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B73C4A142000D0200000004000000010000000042000F010000005842005C0500000004000000030000000042007F0500000004000000000000000042007C0100000030420094070000002466613036303638632D366662312D343265612D623661322D64363664323762313139343300000000

1

Register (Public Key)

In: objectType='00000004', attributes={ CryptographicUsageMask='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:
 30819F300D06092A864886F70D010101050003818D0030818902818100930451C9ECD94F5BB9DA17DD09381BD23BE43EC
 A8C7539F301FC8A8CD5D5274C3E7699DBDC711C97A7AA91E2C50A82BD0B1034F0DF493DEC16362427E58ACCE7F6CE0F9B
 CC617BBD8C90D0094A2703BA0D09EB19D1005F2FB265526AAC75AF32F8BC782CDED2A57F811E03EAF67A944DE5E78413D
 CA8F232D074E6DCEA4CEC9F0203010001

(RSA)

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

42007801000002084200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
 0000000000000042000D0200000004000000010000000042000F01000001C042005C0500000004000000030000000042
 007901000001A8420057050000000400000003000000004200910100000098420008010000003042000A0700000018437
 27970746F67726170686963205573616765204D61736B42000B020000000400000002000000042000801000000584200
 0A07000000044C696E6B000000042000B010000004042004B050000000400000103000000042004C070000002466613
 036303638632D366662312D343265612D623661322D643636643237623131393433000000042006D01000000F0420040
 01000000E8420042050000000400000005000000042004501000000B042004308000000A230819F300D06092A864886F
 70D010101050003818D0030818902818100930451C9ECD94F5BB9DA17DD09381BD23BE43ECA8C7539F301FC8A8CD5D527
 4C3E7699DBDC711C97A7AA91E2C50A82BD0B1034F0DF493DEC16362427E58ACCE7F6CE0F9BCC617BBD8C90D0094A2703B
 A0D09EB19D1005F2FB265526AAC75AF32F8BC782CDED2A57F811E03EAF67A944DE5E78413DCA8F232D074E6DCEA4CEC9F
 0203010001000000000004200280500000004000000040000000042002A02000000040000040000000000

Out: uuidPublicKey

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

- Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A2 (Thu Feb 11 09:49:38 CET 2010)

Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 79cbf228-16df-4fb1-a385-443546935e74

 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
 00000000000000004200920900000008000000004B73C4A242000D0200000004000000010000000042000F010000005842
 005C0500000004000000030000000042007F05000000040000000000000042007C01000000304200940700000024373
 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

 42007801000000F04200770100000038420069010000002042006A020000000400000001000000004200
 6B0200000004000000000000000042000D0200000004000000010000000042000F01000000A842005C0
 5000000040000000D000000004200790100000090420094070000002466613036303638632D36666231
 2D343265612D623661322D64363664323762313139343300000000420008010000005842000A0700000
 0044C696E6B0000000042000B010000004042004B0500000004000001020000000042004C070000002
 437396362663232382D313664662D346662312D613338352D34343335343639333565373400000000

 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-6fbl-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

42007B0100000011042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B73C4A242000D0200000004000000010000000042000F01000000B842005C05000000040000000D0000000042007F05000000040000000000000042007C0100000090420094070000002466613036303638632D366662312D343265612D623661322D64363664323762313139343300000000420008010000005842000A07000000044C696E6B0000000042000B010000004042004B0500000004000001020000000042004C070000002437396362663232382D313664662D346662312D613338352D34343335343639333565373400000000

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

42007801000000F04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F01000000A842005C05000000040000000800000004200790100000090420008010000002842000A070000000B4F626A656374205479706500000000042000B05000000040000000000000420008010000005842000A07000000044C696E6B0000000042000B010000004042004B0500000004000001030000000042004C070000002466613036303638632D366662312D343265612D623661322D64363664323762313139343300000000

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B73C4A242000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F050000000400000000000000042007C01000000304200940700000002437396362663232382D313664662D346662312D613338352D34343335343639333565373400000000

4

Locate (Private Key)

In: attributes={ objectType='PrivateKey', Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } }

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
Tag: Request Header (0x420077), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
Tag: Attribute (0x420008), Type: Structure (0x01), Data:
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Private Key)
Tag: Attribute (0x420008), Type: Structure (0x01), Data:
Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000102 (Public Key Link)
Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: 79cbf228-16df-4fbl-a385-443546935e74

42007801000000F04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F01000000A842005C050000000400000008000000004200790100000090420008010000002842000A070000000B4F626A6563742054797065000000000042000B050000000400000000400000000420008010000005842000A07000000044C696E6B0000000042000B010000004042004B050000000400000102000000042004C0700000002437396362663232382D313664662D346662312D613338352D34343335343639333565373400000000

Out: uuidPrivateKey

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B73C4A342000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F050000000400000000000000042007C0100000030420094070000002466613036303638632D366662312D343265612D623661322D64363664323762313139343300000000

5

Destroy
In: uuidPrivateKey

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

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002466613036303638632D366662312D343265612D623661322D64363664323762313139343300000000

Out: uuidPrivateKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A3 (Thu Feb 11

09:49:39 CET 2010)

- Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 - Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 - Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66d27b11943

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B73C4A342000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F05000000040000000000000042007C0100000030420094070000002466613036303638632D366662312D343265612D623661322D64363664323762313139343300000000

6

Destroy
In: uuidPublicKey

- Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 - Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 - Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 79cbf228-16df-4fb1-a385-443546935e74

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002437396362663232382D313664662D346662312D613338352D34343335343639333565373400000000

Out: uuidPublicKey

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000000


```
00000000000000420092090000008000000004B73C4A342000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F0500000004000000000000000042007C01000000304200940700000024373
96362663232382D313664662D346662312D613338352D34343335343639333565373400000000
```

214

215

216 9 Key Roll-over

217

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

222 9.1 Use-case: Create a Key, Re-key

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

226

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>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</p> <ul style="list-style-type: none"> Tag: Request Header (0x420077), Type: Structure (0x01), Data: <ul style="list-style-type: none"> Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: <ul style="list-style-type: none"> Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: <ul style="list-style-type: none"> Tag: Attribute (0x420008), Type: Structure (0x01), Data: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage <p>Mask</p> <ul style="list-style-type: none"> Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt) Tag: Attribute (0x420008), Type: Structure (0x01), Data: <ul style="list-style-type: none"> 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)

```

42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000011842005C0500000004000000010000000042
007901000001004200570500000004000000020000000042009101000000E8420008010000003042000A0700000017437
27970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200
0A070000001443727970746F67726170686963204C656E677468000000042000B02000000040000000800000000042000
8010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000
0C00000000420008010000003842000A07000000044E616D650000000042000B0100000020420055070000000872656B6
5794B657942005405000000040000000100000000
  
```

Out: objectType='00000002', uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BA (Thu Feb 11 10:07:06 CET 2010)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218

```

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004B73C8BA42000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F050000000400000000000000042007C01000000404200570500000004000
000020000000004200940700000002466623536303733352D656636662D343038352D396530612D65623666313339346332
313800000000
  
```

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)

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000005842005C050000000400000008000000004200790100000040420008010000003842000A07000000044E616D65000000042000B0100000020420055070000000872656B65794B657942005405000000040000000100000000

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B73C8BA42000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F0500000004000000000000000042007C0100000030420094070000002466623536303733352D656636662D343038352D396530612D65623666313339346332313800000000

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

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000008000000004200790100000030420094070000002466623536303733352D656636662D343038352D396530612D65623666313339346332313800000000

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: bf6ccld4-f914-4099-b4d4-453050d8bcf4

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B73C8BB42000D0200000004000000010000000042000F010000005842005C0500000004000000040000000042007F05000000040000000000000042007C0100000030420094070000002462663663633164342D663931342D343039392D623464342D34353330353064386263663400000000

3
Locate
 In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } }

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

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

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000005842005C050000000400000008000000004200790100000040420008010000003842000A07000000044E616D650000000042000B0100000020420055070000000872656B65794B657942005405000000040000000100000000

Out: uuidNewKey

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

- Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BB (Thu Feb 11

10:07:07 CET 2010)

- Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
 - Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 - Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: bf6cc1d4-f914-4099-b4d4-453050d8bcf4

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B73C8BB42000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F05000000040000000000000042007C01000000304200940700000024626636633164342D663931342D343039392D623464342D34353330353064386263663400000000

4

Get Attribute
In: uuidKey, attributeName={'Name'}

- Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 - Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
 - Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218
 - Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B000000004200790100000040420094070000002466623536303733352D656636662D343038352D396530612D6562366631333934633231380000000042000A07000000044E616D6500000000

Out: uuidKey

- Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 - Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BB (Thu Feb 11 10:07:07 CET 2010)
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
 - Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 - Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B73C8BB42000D0200000004000000010000000042000F010000005842005C05000000040000000B0000000042007F0500000004000000000000000042007C0100000030420094070000002466623536303733352D656636662D343038352D396530612D65623666313339346332313800000000

5

Get (symmetric key)

In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
Tag: Request Header (0x420077), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002466623536303733352D656636662D343038352D396530612D65623666313339346332313800000000

Out: objectType = '00000002', uuidKey, symmetricKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BB (Thu Feb 11 10:07:07 CET 2010)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218
Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
Tag: Key Block (0x420040), Type: Structure (0x01), Data:
Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
Tag: Key Value (0x420045), Type: Structure (0x01), Data:
Tag: Key Material (0x420043), Type: Octet String (0x08), Data: BC25617991C49D06536008D076017462
Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

	<pre> 42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040 0000000000000004200920900000008000000004B73C8BB42000D0200000004000000010000000042000F01000000C842 005C05000000040000000A0000000042007F050000000400000000000000042007C01000000A04200570500000004000 0000200000000420094070000002466623536303733352D656636662D343038352D396530612D65623666313339346332 31380000000042008F0100000058420040010000005042004205000000040000000100000000420045010000001842004 30800000010BC25617991C49D06536008D0760174624200280500000004000000030000000042002A0200000004000000 8000000000 </pre>
6	<p>Destroy 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: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-eb6f1394c218</p> <pre> 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040 00000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000140000000042 00790100000030420094070000002466623536303733352D656636662D343038352D396530612D6562366631333934633 23138000000000 </pre> <p>Out: uuidKey</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: 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</p> <pre> 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040 0000000000000004200920900000008000000004B73C8BC42000D0200000004000000010000000042000F010000005842 005C0500000004000000140000000042007F050000000400000000000000042007C01000000304200940700000024666 23536303733352D656636662D343038352D396530612D656236663133393463323138000000000 </pre>
7	<p>Destroy In: uuidNewKey</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: bf6cc1d4-f914-4099-b4d4-453050d8bcf4

```

```

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000042
00790100000030420094070000002462663663633164342D663931342D343039392D623464342D3435333035306438626
3663400000000

```

Out: uuidNewKey

```

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

```

```

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000004200920900000008000000004B73C8BC42000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F050000000400000000000000042007C01000000304200940700000024626
63663633164342D663931342D343039392D623464342D34353330353064386263663400000000

```

227

228

229 9.2 Use-case: Existing Key Expired, Re-key with Same lifecycle

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

238

Time	Client A
0	<p>Create (symmetric key)</p> <p>In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C' }</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</p> <ul style="list-style-type: none"> Tag: Request Header (0x420077), Type: Structure (0x01), Data: <ul style="list-style-type: none"> Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: <ul style="list-style-type: none"> Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: <ul style="list-style-type: none"> Tag: Attribute (0x420008), Type: Structure (0x01), Data: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: <ul style="list-style-type: none"> Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) <p>42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000011842005C0500000004000000010000000042007901000001004200570500000004000000020000000042009101000000E8420008010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000A0700000001443727970746F67726170686963204C656E6774680000000042000B020000000400000008000000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000040000000C00000000420008010000003842000A07000000044E616D650000000042000B0100000020420055070000000872656B65794B657942005405000000040000000100000000</p> <p>Out: objectType='00000002', uuidKey</p> <p>Tag: Response Message (0x42007B), Type: Structure (0x01), Data:</p> <ul style="list-style-type: none"> Tag: Response Header (0x42007A), Type: Structure (0x01), Data: <ul style="list-style-type: none"> Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: <ul style="list-style-type: none"> 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

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B73FFC742000D0200000004000000010000000042000F010000006842005C0500000004000000010000000042007F050000000400000000000000042007C01000000404200570500000004000000020000000420094070000002466626335663365352D343862662D343239342D623735342D30353735613431643933623600000004200808010000002842000A070000000F41637469766174696F6E20446174650042000B0900000008000000004992CC4742000F010000009042005

1 Add Activation Date, Deactivation Date attributes based on Timestamp in previous response (batch)
 In: uuidKey, attribute={ ActivationDate=' <Timestamp in previous response – 365 days>' }
 In: uuidKey, attribute={ DeactivationDate='<Timestamp in previous response + 2 minutes>' }

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BAC4A9CECC650259

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

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6

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

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

Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004992CC47 (Wed Feb 11 14:01:59 CET 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: Request Payload (0x420079), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6

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

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

Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B74003F (Thu Feb 11 14:03:59 CET 2010)

42007801000001784200770100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000000420010060000000800000000000000142000D0200000004000000020000000042000F010000008842005C05000000040000000D000000004200930800000008BAC4A9CECC6502594200790100000060420094070000002466626335663365352D343862662D343239342D623735342D30353735613431643933623600000004200808010000002842000A070000000F41637469766174696F6E20446174650042000B0900000008000000004992CC4742000F010000009042005

C05000000040000000D000000004200930800000008582C952324F4552F4200790100000068420094070000002466626335663365352D343862662D343239342D623735342D30353735613431643933623600000000420008010000003042000A0700000011446561637469766174696F6E2044617465000000000000042000B0900000008000000004B74003F

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

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

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73FFC7 (Thu Feb 11 14:01:59 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BAC4A9CECC650259

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6

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

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

Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004992CC47 (Wed Feb 11 14:01:59 CET 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)

42007B010000019842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B73FFC742000D0200000004000000020000000042000F010000009842005C050000000400000000D000000004200930800000008BAC4A9CECC65025942007F0500000004000000000000000042007C0100000060420094070000002466626335663365352D343862662D343239342D623735342D30353735613431643933623600000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B0900000008000000004992CC4742000F01000000A042005C05000000040000000D000000004200930800000008582C952324F4552F42007F05000000040000000000000042007C01000000068420094070000002466626335663365352D343862662D343239342D623735342D3035373561343164393362360000000420008010000003042000A0700000011446561637469766174696F6E2044617465000000000000042000B0900000008000000004B74003F

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

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000005842005C050000000400000000B000000004200790100000040420094070000002466626335663365352D343862662D343239342D623735342D3035373561343164393362360000000042000A07000000055374617465000000

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)

42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000042009209000000800000004B73FFC742000D0200000004000000010000000042000F010000008042005C050000000400000000B0000000042007F050000000400000000000000042007C0100000058420094070000002466626335663365352D343862662D343239342D623735342D3035373561343164393362360000000420008010000002042000A0700000005537461746500000042000B05000000040000000200000000

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

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B000000004200790100000040420094070000002466626335663365352D343862662D343239342D623735342D3035373561343164393362360000000042000A07000000055374617465000000

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

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

42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74004042000D0200000004000000010000000042000F010000008042005C05000000040000000B0000000042007F05000000040000000000000042007C0100000058420094070000002466626335663365352D343862662D343239342D623735342D3035373561343164393362360000000042000801000000204200A0700000005537461746500000042000B05000000040000000300000000

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

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

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000005842005C0500000004000000040000000042
00790100000040420094070000002466626335663365352D343862662D343239342D623735342D3035373561343164393
36236000000004200580A000000004FE747E0000000000

Out: uuidNewKey

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004B74004042000D0200000004000000010000000042000F010000005842
005C0500000004000000040000000042007F050000000400000000000000000042007C01000000304200940700000024333
83936303262312D636130322D346333632D623561332D63333738396537663263393200000000

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

42007801000000C84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F0100000008042005C050000000400000000B0000000042
00790100000068420094070000002433383936303262312D636130322D346333632D623561332D6333373839653766326
339320000000042000A070000000F41637469766174696F6E20446174650042000A0700000001144656163746976617469
6F6E204461746500000000000000

Out: uuidNewKey, attribute={' ActivationDate=' <Value of ActivationTime in existing key + 65 days>',

DeactivationDate='< Value of DeactivationDate of existing key + 65 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)

42007B0100000011842007A01000000048420069010000002042006A0200000004000000010000000042006B0200000000400000000000004200920900000008000000004B74004042000D0200000004000000010000000042000F01000000C042005C05000000040000000B0000000042007F050000000400000000000000042007C0100000098420094070000002433383936303262312D636130322D346333632D623561332D63333738396537663263393200000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B09000000080000000049E87DC64200080100000003042000A0700000011446561637469766174696F6E2044617465000000000000042000B0900000008000000004BC9B1BE

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

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000004000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B000000004200790100000040420094070000002433383936303262312D636130322D346333632D623561332D6333373839653766326339320000000042000A07000000055374617465000000

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)

42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74004042000D0200000004000000010000000042000F0100000008042005C05000000040000000B0000000042007F05000000040000000000000042007C0100000058420094070000002433383936303262312D636130322D346333632D623561332D63333738396537663263393200000000420008010000002042000A0700000005537461746500000042000B05000000040000000200000000

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

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000014000000004200790100000030420094070000002466626335663365352D343862662D343239342D623735342D30353735613431643933623600000000

Out: uuidKey

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

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11 14:04:00 CET 2010)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-0575a41d93b6

 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
 00000000000000004200920900000008000000004B74004042000D0200000004000000010000000042000F010000005842
 005C0500000004000000140000000042007F050000000400000000000000042007C01000000304200940700000024666
 26335663365352D343862662D343239342D623735342D30353735613431643933623600000000

8

Revoke (symmetric key as cessation of operation) and Destroy

In (header): batchOrderOption='TRUE'
 In: uuidKey, revocationReasonCode='6'
 In: uuidNewKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7012417AA1B7394B
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92
 Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:
 Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000006 (Cessation of Operation)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3F8F4F1759704555
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92

 42007801000001284200770100000048420069010000002042006A0200000004000000010000000042006B02000000040
 0000000000000000420010060000000800000000000000142000D0200000004000000020000000042000F010000007042
 005C0500000004000000130000000042009308000000087012417AA1B7394B42007901000000484200940700000024333
 83936303262312D636130322D346333632D623561332D6333373839653766326339320000000042008101000000104200
 820500000004000000060000000042000F010000005842005C0500000004000000140000000042009308000000083F8F4
 F17597045554200790100000030420094070000002433383936303262312D636130322D346333632D623561332D633337
 38396537663263393200000000

	<p>Out: uuidNewKey</p> <p>Out: uuidNewKey</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: 0x000000004B740040 (Thu Feb 11 14:04:00 CET 2010)</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: 0x00000013 (Revoke)</p> <p> Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7012417AA1B7394B</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: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92</p> <p> Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:</p> <p> Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)</p> <p> Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3F8F4F1759704555</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: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92</p> <p>42007B010000013042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74004042000D0200000004000000020000000042000F010000006842005C0500000004000000013000000042009308000000087012417AA1B7394B42007F05000000040000000000000042007C0100000030420094070000002433383936303262312D636130322D346333632D623561332D633337383965376632633932000000042000F010000006842005C0500000004000000014000000042009308000000083F8F4F175970455542007F05000000040000000000000042007C0100000030420094070000002433383936303262312D636130322D346333632D623561332D63333738396537663263393200000000</p>
--	---

239

240 **9.3 Use-case: Existing Key Compromised, Re-key with same lifecycle**

241 Create a new symmetric key with the *Activation Date* in the past. Do a Get Attribute operation on the

242 State attribute to verify the key is “Active”. Then revoke the key as compromised, verify that the state has

243 changed to “Compromised”. Create a replacement key using Re-key with the offset set to ‘0’ to indicate

244 that the times are to be copied from the existing key. Do a Get Attribute operation to verify that the state

245 of the new key is “Active”. To clean up, both keys are deleted.

246

Time	Client A
0	<p>Create (symmetric key)</p> <p>In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='rekeyKey', NameType='00000001' }, ActivationDate='<NOW>' }</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</p>

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)

```
42007801000001904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000014842005C0500000004000000010000000042
00790100000130420057050000000400000002000000004200910100000118420008010000003042000A0700000017437
27970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200
0A070000001443727970746F67726170686963204C656E677468000000042000B02000000040000000800000000042000
8010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000
0C00000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B09000000080000000
04B741047420008010000003842000A07000000044E616D650000000042000B0100000020420055070000000872656B65
794B657942005405000000040000000100000000
```

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

 42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
 000000000000004200920900000008000000004B74104842000D020000000400000001000000004200F010000006842
 005C0500000004000000010000000042007F05000000040000000000000042007C01000000404200570500000004000
 0000200000000420094070000002465656137343262342D393665642D343233382D616664322D35333138396337396637
 383100000000

1

Get Attribute
In: uuidKey, attributeName={'State'}

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

 42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
 00000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B0000000042
 00790100000040420094070000002465656137343262342D393665642D343233382D616664322D3533313839633739663
 738310000000042000A07000000055374617465000000

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

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741048 (Thu Feb 11 15:12:24 CET 2010)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781
 Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

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

42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74104842000D0200000004000000010000000042000F010000008042005C05000000040000000B0000000042007F050000000400000000000000042007C0100000058420094070000002465656137343262342D393665642D343233382D616664322D3533313839633739663738310000000042000801000000204200A0700000005537461746500000042000B05000000040000000200000000

2

Revoke (symmetric key as compromised)
In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceDate='<NOW>'

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

- Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
 - Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781
 - Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:
 - Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000002 (Key Compromise)
 - Tag: Compromise Occurrence Date (0x420021), Type: Date-Time (0x09), Data: 0x000000004B741048 (Thu Feb 11 15:12:24 CET 2010)

42007801000000B84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000007042005C0500000004000000013000000004200790100000058420094070000002465656137343262342D393665642D343233382D616664322D3533313839633739663738310000000042008101000000104200820500000004000000020000000042002109000000080000000004B741048

Out: uuidKey

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

- Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11 15:12:25 CET 2010)
- Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

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

- Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
- Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
- Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74104942000D0200000004000000010000000042000F010000005842005C05000000040000000130000000042007F050000000400000000000000042007C01000000304200940700000024656

	56137343262342D393665642D343233382D616664322D35333138396337396637383100000000
3	<p>Get Attribute In: uuidKey, attributeName={'State'}</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: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State</p> <p>42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B000000004200790100000040420094070000002465656137343262342D393665642D343233382D616664322D3533313839633739663738310000000042000A07000000055374617465000000</p> <p>Out: uuidKey, attribute={ State='Compromised' }</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: 0x000000004B741049 (Thu Feb 11 15:12:25 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-53189c79f781 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Compromised)</p> <p>42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74104942000D0200000004000000010000000042000F010000008042005C05000000040000000B0000000042007F05000000040000000000000042007C0100000058420094070000002465656137343262342D393665642D343233382D616664322D35333138396337396637383100000000420008010000002042000A0700000005537461746500000042000B050000000400000000400000000</p>
4	<p>Rekey In: uuidKey</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: eea742b4-96ed-4238-afd2-53189c79f781

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000400000004200790100000030420094070000002465656137343262342D393665642D343233382D616664322D35333138396337396637383100000000

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B74104942000D0200000004000000010000000042000F010000005842005C0500000004000000040000000042007F05000000040000000000000042007C0100000030420094070000002461643363623737342D643030642D343539312D613633342D36656133366138303138323400000000

5	<p>Get Attribute In: uuidNewKey, attributeName={'State'}</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: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-</p>
---	--

6ea36a801824

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

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B000000004200790100000040420094070000002461643363623737342D643030642D343539312D613633342D3665613336613830313832340000000042000A07000000055374617465000000

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)

42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74104942000D0200000004000000010000000042000F010000008042005C05000000040000000B0000000042007F05000000040000000000000042007C0100000058420094070000002461643363623737342D643030642D343539312D613633342D3665613336613830313832340000000042000801000000204200A0700000005537461746500000042000B05000000040000000200000000

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

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000014000000004200790100000030420094070000002465656137343262342D393665642D343233382D616664322D35333138396337396637383100000000

Out: uuidKey

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74104942000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F050000000400000000000000042007C0100000030420094070000002465656137343262342D393665642D343233382D616664322D35333138396337396637383100000000

7

Revoke (symmetric key as cessation of operation) and Destroy

In (header): batchOrderOption='TRUE'

In: uuidNewKey, revocationReasonCode='6'

In: uuidNewKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7131695CF636735E
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-6ea36a801824
 Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:
 Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000006 (Cessation of Operation)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 1845BCBBF09B5A66
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-6ea36a801824

```
42007801000001284200770100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000420010060000000800000000000000142000D0200000004000000020000000042000F010000007042
005C0500000004000000130000000042009308000000087131695CF636735E42007901000000484200940700000024616
43363623737342D643030642D343539312D613633342D3665613336613830313832340000000042008101000000104200
820500000004000000060000000042000F010000005842005C050000000400000014000000004200930800000081845B
CBBF09B5A664200790100000030420094070000002461643363623737342D643030642D343539312D613633342D366561
33366138303138323400000000
```

Out: uuidNewKey

Out: uuidNewKey

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

42007B010000013042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004B74104942000D0200000004000000020000000042000F010000006842
005C0500000004000000130000000042009308000000087131695CF636735E42007F0500000004000000000000000420
07C0100000030420094070000002461643363623737342D643030642D343539312D613633342D36656133366138303138
32340000000042000F010000006842005C050000000400000014000000004200930800000081845BCBBF09B5A6642007
F050000000400000000000000042007C0100000030420094070000002461643363623737342D643030642D343539312D
613633342D36656133366138303138323400000000
```

247

248

249 9.4 Use-case: Create key, Re-key with new lifecycle

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

253

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:
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)

42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000011842005C0500000004000000010000000042
007901000001004200570500000004000000020000000042009101000000E8420008010000003042000A0700000017437
27970746F6772617068696320416C676F726974686D042000B050000004000000030000000042000801000000304200
0A070000001443727970746F67726170686963204C656E677468000000042000B0200000004000000800000000042000
8010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000
0C00000000420008010000003842000A07000000044E616D65000000042000B0100000020420055070000000872656B6
5794B657942005405000000040000000100000000

Out: objectType='00000002', uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742475 (Thu Feb 11
16:38:29 CET 2010)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
 000000000000004200920900000008000000004B74247542000D020000000400000001000000004200F010000006842
 005C0500000004000000010000000042007F05000000040000000000000042007C01000000404200570500000004000
 0000200000000420094070000002466303334323539302D663738612D346433342D613266342D34643666633835613536
 656600000000

1	<p>Locate</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>42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040 0000000000000042000D020000000400000001000000004200F010000005842005C0500000004000000080000000042 007901000000040420008010000003842000A07000000044E616D650000000042000B01000000204200550700000008726 56B65794B657942005405000000040000000100000000</p> <p>Out: uuidKey</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: 0x000000004B742476 (Thu Feb 11 16:38:30 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-</p>
---	--

4d6fc85a56ef
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B74247642000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F050000000400000000000000042007C0100000030420094070000002466303334323539302D663738612D346433342D613266342D34643666633835613536656600000000

2
Rekey
In: uuidKey, attributes={ ActivationDate='000000043B7B630', ProcessStartDate='000000043B7B630', ProtectStopDate='00000005E0C7BB0', DeactivationDate='00000005E0C7BB0' }

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)

42007801000001704200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000012842005C0500000004000000040000000042009101000000D8420008010000002842000A070000000F41637469766174696F6E20446174650042000B09000000080000000043B7B630420008010000003042000A070000001250726F63657373205374617274204461746500000000042000B09000000080000000043B7B630420008010000003042000A070000001150726F746563742053746F702044617465000000000000042000B090000000800000005E0C7BB0420008010000003042000A0700000011446561637469766174696F6E2044617465000000000000042000B090000000800000005E0C7BB0

Out: uuidNewKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

- Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742477 (Thu Feb 11 16:38:31 CET 2010)

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

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

- Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
- Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
- Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74247742000D0200000004000000010000000042000F010000005842005C0500000004000000040000000042007F050000000400000000000000042007C0100000030420094070000002461336661366535632D313339372D346162342D396431322D66663666666161373566626400000000

3

Get Attribute

In: uuidKey, attributeName={'Name'}

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

- Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
 - Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef
 - Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B000000004200790100000040420094070000002466303334323539302D663738612D346433342D613266342D3464366663383561353665660000000042000A07000000044E616D6500000000

Out: uuidKey

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

- Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742477 (Thu Feb 11 16:38:31 CET 2010)
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
 - Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

	<p>Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef</p> <p>42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74247742000D0200000004000000010000000042000F010000005842005C05000000040000000B0000000042007F050000000400000000000000042007C0100000030420094070000002466303334323539302D663738612D346433342D613266342D34643666633835613536656600000000</p>
4	<p>Get Attribute</p> <p>In: uuidKey, attributeName={ 'ActivationDate', 'ProcessStartDate', 'ProtectStopDate', 'DeactivationDate' }</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: 0x0000000B (Get Attributes)</p> <p>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p>Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Process Start Date</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date</p> <p>Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date</p> <p>42007801000001084200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F01000000C042005C05000000040000000B0000000042007901000000A8420094070000002461336661366535632D313339372D346162342D396431322D6666366666616137356662640000000042000A070000000F41637469766174696F6E20446174650042000A070000001250726F63657373205374617274204461746500000000000042000A070000001150726F746563742053746F7020446174650000000000000042000A0700000011446561637469766174696F6E204461746500000000000000</p> <p>Out: uuidKey, attribute={ ActivationDate='000000043B7B630', ProcessStartDate='000000043B7B630', ProtectStopDate='00000005E0C7BB0', DeactivationDate='00000005E0C7BB0' }</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: 0x000000004B742477 (Thu Feb 11 16:38:31 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: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd</p>

Tag: Attribute (0x420008), Type: Structure (0x01), Data:
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
 Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000043B7B630 (Sun Jan 01 12:00:00 CET 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: 0x0000000043B7B630 (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: 0x000000005E0C7BB0 (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: 0x000000005E0C7BB0 (Wed Jan 01 12:00:00 CET 2020)

```
42007B010000018842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004B74247742000D0200000004000000010000000042000F010000013042
005C050000000400000000B0000000042007F050000000400000000000000042007C01000001084200940700000024613
36661366535632D313339372D346162342D396431322D6666366666616137356662640000000042000801000000284200
0A0700000000F41637469766174696F6E20446174650042000B09000000080000000043B7B630420008010000003042000
A070000001250726F6365737320537461727420446174650000000000042000B09000000080000000043B7B630420008
010000003042000A070000001150726F746563742053746F70204461746500000000000042000B09000000080000000
05E0C7BB0420008010000003042000A0700000011446561637469766174696F6E204461746500000000000042000B09
00000008000000005E0C7BB0
```

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

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

```
42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042
00790100000040420008010000003842000A07000000044E616D65000000042000B01000000204200550700000008726
56B65794B657942005405000000040000000100000000
```

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B74247742000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F05000000040000000000000042007C0100000030420094070000002461336661366535632D313339372D346162342D396431322D66663666666161373566626400000000

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

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000001400000000420094070000002466303334323539302D663738612D346433342D613266342D34643666633835613536656600000000

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004B74247842000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F050000000400000000000000042007C01000000304200940700000024663
03334323539302D663738612D346433342D613266342D34643666633835613536656600000000

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

42007801000001284200770100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420010060000000800000000000000142000D0200000004000000020000000042000F010000007042
005C0500000004000000130000000042009308000000083DC816BB39869D0742007901000000484200940700000024613
36661366535632D313339372D346162342D396431322D666636666661613735666264000000042008101000000104200
820500000004000000060000000042000F010000005842005C05000000040000001400000000420093080000000832B51
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: 0x000000004B742478 (Thu Feb 11
16:38:32 CET 2010)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3DC816BB39869D07
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-
ff6ffaa75fbd
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 32B517312FD5B558
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-
ff6ffaa75fbd

42007B010000013042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000004200920900000008000000004B74247842000D0200000004000000020000000042000F010000006842
005C0500000004000000130000000042009308000000083DC816BB39869D0742007F050000000400000000000000420
07C0100000030420094070000002461336661366535632D313339372D346162342D396431322D66663666666161373566
62640000000042000F010000006842005C05000000040000001400000000420093080000000832B517312FD5B55842007
F050000000400000000000000042007C0100000030420094070000002461336661366535632D313339372D346162342D
396431322D66663666666161373566626400000000

```

254

255

256 9.5 Use-case: Obtain Lease for Expired Key

- 257 Create a symmetric key with a specific name and obtain a lease. Revoke the key with state
- 258 "Compromised" and re-key the key. Try to obtain a lease on the old key which fails. Locate the new key
- 259 with the original name. Get the new key and obtain a lease.
- 260

Time	Client
0	<p>Client A:</p> <p>Create (symmetric key)</p> <p>In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue=' rekeyKey', NameType='00000001' }, ActivationDate='<NOW>' }</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: 0x00000001 (Create)</p>

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

Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:

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

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

Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)

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

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

Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)

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

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

Mask

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

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

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

Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:

Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey

Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

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

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

Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B74262C (Thu Feb 11 16:45:48 CET 2010)

```
42007801000001904200770100000038420069010000002042006A0200000004000000010000000042006B020000000040
0000000000000042000D0200000004000000010000000042000F010000014842005C0500000004000000010000000042
0079010000013042005705000000040000000200000004200910100000118420008010000003042000A0700000017437
27970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200
0A070000001443727970746F67726170686963204C656E677468000000042000B0200000004000000080000000042000
8010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000
0C000000042000801000003842000A0700000044E616D65000000042000B0100000020420055070000000872656B6
5794B65794200540500000004000000010000000420008010000002842000A070000000F41637469766174696F6E2044
6174650042000B0900000008000000004B74262C
```

Out: objectType='00000002', uuidKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262D (Thu Feb 11 16:45:49 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74262D42000D0200000004000000010000000042000F010000006842005C0500000004000000010000000042007F050000000400000000000000042007C01000000404200570500000004000002000000004200940700000002463613336386533332D646333642D346337632D386636642D3236323839356263331636500000000

1

Client A:
Get (symmetric key)
In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A0000000042007901000000304200940700000002463613336386533332D646333642D346337632D386636642D3236323839356263331636500000000

Out: objectType = '00000002', uuidKey, symmetricKey

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

Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74262D42000D0200000004000000010000000042000F01000000C842005C05000000040000000A0000000042007F050000000400000000000000042007C01000000A042005705000000040000000000000420094070000002463613336386533332D646333642D346337632D386636642D323632383935626333163650000000042008F010000005842004001000000504200420500000004000000010000000042004501000000184200430800000010F43C7798AACB22B1411A8773C199708B4200280500000004000000030000000042002A02000000040000008000000000

2

Client A:
Obtain Lease
In: uuidKey

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

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000001000000000420094070000002463613336386533332D646333642D346337632D386636642D3236323839356263331636500000000

Out: uuidKey, leaseTime, lastChangeDate

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262E (Thu Feb 11 16:45:50 CET 2010)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce
Tag: Lease Time (0x420049), Type: Interval (0x0A), Data: 0x00000010
Tag: Last Change Date (0x420048), Type: Date-Time (0x09), Data: 0x000000004B74262D (Thu Feb 11 16:45:49 CET 2010)

42007B01000000D042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74262E42000D0200000004000000010000000042000F010000007842

005C0500000004000000100000000042007F050000000400000000000000042007C01000000504200940700000024636
13336386533332D646333642D346337632D386636642D323632383935626333316365000000004200490A000000040000
0010000000004200480900000008000000004B74262D

3
Client B:
Revoke (symmetric key as compromised)
In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceDate='<NOW>'

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce
 Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:
 Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000002 (Key Compromise)
 Tag: Compromise Occurrence Date (0x420021), Type: Date-Time (0x09), Data: 0x000000004B74262E (Thu Feb 11 16:45:50 CET 2010)

42007801000000B84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000042000D0200000004000000010000000042000F010000007042005C05000000040000000130000000042
00790100000058420094070000002463613336386533332D646333642D346337632D386636642D3236323839356263333
16365000000004200810100000010420082050000000400000002000000004200210900000008000000004B74262E

Out: uuidKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262E (Thu Feb 11 16:45:50 CET 2010)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000004200920900000008000000004B74262E42000D0200000004000000010000000042000F010000005842
005C0500000004000000130000000042007F050000000400000000000000042007C01000000304200940700000024636
13336386533332D646333642D346337632D386636642D32363238393562633331636500000000

4
Client B:

Rekey

In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
Tag: Request Header (0x420077), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000004000000004200790100000030420094070000002463613336386533332D646333642D346337632D386636642D32363238393562633331636500000000

Out: uuidNewKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)
Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B74262F42000D0200000004000000010000000042000F010000005842005C0500000004000000040000000042007F05000000040000000000000042007C0100000030420094070000002435396662663831642D353734662D346634662D393538312D37373835646335393366356600000000

5

Client A:
Obtain Lease
In: uuidKey

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

Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000100000000042007901000000304200940700000002463613336386533332D646333642D346337632D386636642D32363238393562633331636500000000

Out: Operation Failed, Permission Denied

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)
 Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x0000000C (Permission Denied)
 Tag: Result Message (0x42007D), Type: Text String (0x07), Data: CO is in state Compromised, no lease given

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74262F42000D0200000004000000010000000042000F010000006842005C0500000004000000100000000042007F0500000004000000010000000042007E05000000040000000C0000000042007D070000002A434F20697320696E20737461746520436F6D70726F6D697365642C206E6F206C6561736520676976656E000000000000

6 Client A:
 Locate (symmetric key)
 In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } }

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

Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000005842005C050000000400000008000000004200790100000040420008010000003842000A07000000044E616D65000000042000B0100000020420055070000000872656B65794B657942005405000000040000000100000000

Out: uuidNewKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B74262F42000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F0500000004000000000000000042007C0100000030420094070000002435396662663831642D353734662D346634662D393538312D373738356463353933635660000000

7

Client A:

Get (symmetric key)

In: uuidNewKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)

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

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002435396662663831642D353734662D346634662D393538312D37373835646335393363566000000000

Out: objectType = '00000002', uuidNewKey, newSymmetricKey

```

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11
16:45:51 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-
7785dc593f5f
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data:
173E9499F7C573712AFB9883B5DF2BCE
            Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003
(AES)
            Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004B74262F42000D0200000004000000010000000042000F01000000C842
005C05000000040000000A0000000042007F050000000400000000000000042007C01000000A04200570500000004000
0000200000000420094070000002435396662663831642D353734662D346634662D393538312D37373835646335393366
35660000000042008F0100000058420040010000005042004205000000040000000100000000420045010000001842004
30800000010173E9499F7C573712AFB9883B5DF2BCE4200280500000004000000030000000042002A0200000004000000
8000000000

```

8

Client A:
Obtain Lease
In: uuidNewKey

```

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
      Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-
7785dc593f5f

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000010000000042
00790100000030420094070000002435396662663831642D353734662D346634662D393538312D37373835646335393366

```

635660000000

Out: uuidNewKey, leaseTime, lastChangeDate

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f
 Tag: Lease Time (0x420049), Type: Interval (0x0A), Data: 0x00000000
 Tag: Last Change Date (0x420048), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)

42007B01000000D042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B74262F42000D0200000004000000010000000042000F010000007842005C0500000004000000100000000042007F05000000040000000000000042007C0100000050420094070000002435396662663831642D353734662D346634662D393538312D37373835646335393363566000000004200490A000000040000000000004200480900000008000000004B74262F

9

**Client A:
Destroy
In: uuidKey**

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002463613336386533332D646333642D346337632D386636642D32363238393562633331636500000000

Out: uuidKey

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

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000042009209000000080000000004B74262F42000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F050000000400000000000000042007C0100000030420094070000002463613336386533332D646333642D346337632D386636642D32363238393562633331636500000000

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

- Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
 - Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3748B9E243205BA7
- Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f
 - Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:
 - Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000006 (Cessation of Operation)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
 - Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 04EAF416D0BEB50D
- Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 - Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f

42007801000001284200770100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000042001006000000080000000000000142000D0200000004000000020000000042000F010000007042005C0500000004000000130000000042009308000000083748B9E243205BA742007901000000484200940700000024353

96662663831642D353734662D346634662D393538312D373738356463353933663566000000042008101000000104200820500000004000000060000000042000F010000005842005C05000000040000001400000000420093080000000804EAF416D0BEB50D4200790100000030420094070000002435396662663831642D353734662D346634662D393538312D37373835646335393366356600000000

Out: uuidNewKey

Out: uuidNewKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3748B9E243205BA7

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 04EAF416D0BEB50D

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f

42007B010000013042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B74262F42000D0200000004000000020000000042000F010000006842005C0500000004000000130000000042009308000000083748B9E243205BA742007F0500000004000000000000000042007C0100000030420094070000002435396662663831642D353734662D346634662D393538312D373738356463353933663566000000042000F010000006842005C05000000040000001400000000420093080000000804EAF416D0BEB50D42007F050000000400000000000000042007C0100000030420094070000002435396662663831642D353734662D346634662D393538312D37373835646335393366356600000000

261

262 10 Archival

263

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

267 10.1 Use-case: Create a Key, Archive and Recover it

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

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>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: 0x00000001 (Create)</p> <p> Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p> Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</p> <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</p> <p>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: archiveKey</p> <p> Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)</p> <p>42007801000001684200770100000038420069010000002042006A020000000400000001000000042006B0200000004000000000000042000D020000000400000001000000042000F010000012042005C05000000040000000100000000420009101000000F0420008010000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000A070000001443727970746F67726170686963204C656E677468000000042000B020000000400000080000000000420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000040000000C00000000420008010000004042000A07000000044E616D65000000042000B010000002842005507000000A617263686976654B65790000000000042005405000000040000000100000000</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>

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FA3 (Fri Feb 12 10:30:11 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B751FA342000D0200000004000000010000000042000F010000006842005C0500000004000000010000000042007F050000000400000000000000042007C01000000404200570500000004000000020000000420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000

1
Locate
 In: attributes={ Name={ NameValue='archiveKey', NameType='00000001' } }

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

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

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

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

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

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

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

Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:

Tag: Name Value (0x420055), Type: Text String (0x07), Data: archiveKey

Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007801000000D84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000009042005C050000000400000008000000004200790100000078420008010000002842000A070000000B4F626A656374205479706500000000042000B050000000400000000200000000420008010000004042000A07000000044E616D65000000042000B0100000028420055070000000A617263686976654B657900000000000042005405000000040000000100000000

Out: uuidKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FA6 (Fri Feb 12 10:30:14 CET 2010)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f

 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
 000000000000004200920900000008000000004B751FA642000D0200000004000000010000000042000F010000005842
 005C0500000004000000080000000042007F05000000040000000000000042007C01000000304200940700000024306
 43535323136302D666230342D346637632D386137332D66656639303562323163306600000000

2

Get (symmetric key)

In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f

 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
 0000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000000A0000000042
 00790100000030420094070000002430643535323136302D666230342D346637632D386137332D6665663930356232316
 33066000000000

Out: objectType = '00000002', uuidKey, symmetricKey

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FA7 (Fri Feb 12 10:30:15 CET 2010)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f

Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:

Tag: Key Block (0x420040), Type: Structure (0x01), Data:

Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001

Tag: Key Value (0x420045), Type: Structure (0x01), Data:

Tag: Key Material (0x420043), Type: Octet String (0x08), Data: C3200B1291BA648DB9089DED3073DE74

Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)

Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B751FA742000D0200000004000000010000000042000F01000000C842005C05000000040000000A0000000042007F050000000400000000000000042007C01000000A042005705000000040000000000000420094070000002430643535323136302D666230342D346637632D386137332D666566393035623231633066000000042008F0100000058420040010000005042004205000000400000001000000042004501000000184200430800000010C3200B1291BA648DB9089DED3073DE744200280500000004000000030000000042002A02000000040000000800000000

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

42007801000000A04200770100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000420092090000000800000000000000142000D0200000004000000010000000042000F01000000C842005C0500000004000000015000000004200790100000030420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000

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)

	<p>Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Operation Pending)</p> <p>Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: F17893DB51652969</p> <p>42007B010000008842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B751FA742000D0200000004000000010000000042000F010000003042005C0500000004000000150000000042007F050000000400000002000000004200060800000008F17893DB51652969</p>
4	<p>Poll*</p> <p>In: asynchronousCorrelationValue</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: 0x0000001A (Poll)</p> <p>Tag: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p>Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: F17893DB51652969</p> <p>42007801000000704200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000002842005C050000000400000001A0000000042007901000000104200060800000008F17893DB51652969</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: 0x000000004B751FAA (Fri Feb 12 10:30:18 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: 0x00000015 (Archive)</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>42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B751FAA42000D0200000004000000010000000042000F010000005842005C0500000004000000150000000042007F0500000004000000000000000042007C0100000030420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000</p>
5	<p>Get (symmetric key)</p> <p>In: uuidKey</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: 0x0000000A (Get)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
 000000000000042000D02000000400000001000000004200F010000004842005C05000000040000000A0000000042
 00790100000030420094070000002430643535323136302D666230342D346637632D386137332D6665663930356232316
 3306600000000

Out: Operation Failed, Object Archived

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x00000004B751FAC (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

42007B01000000A842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
 00000000000004200920900000008000000004B751FAC42000D020000000400000001000000004200F010000005042
 005C0500000004000000A0000000042007F0500000004000000010000000042007E05000000040000000D00000000420
 07D07000000124F626A65637420697320617263686976656400000000000

6

Get Attribute (Archive Date)
In: uuidKey, attributeName='ArchiveDate'

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

fef905b21c0f

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

42007801000000A84200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000006042005C05000000040000000B0000000004200790100000048420094070000002430643535323136302D666230342D346637632D386137332D666566393035623231633066000000042000A070000000C41726368697665204461746500000000

Out: uuidKey, attribute={ ArchiveDate }

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAC (Fri Feb 12 10:30:20 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f

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

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

Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B751FAA (Fri Feb 12 10:30:18 CET 2010)

42007B01000000E042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000004200920900000008000000004B751FAC42000D0200000004000000010000000042000F010000008842005C05000000040000000B0000000042007F050000000400000000000000042007C0100000060420094070000002430643535323136302D666230342D346637632D386137332D666566393035623231633066000000042000A070000000C417263686976652044617465000000042000B0900000008000000004B751FAA

7

Locate

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

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

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

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

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

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

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

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

```
42007801000000D84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000009042005C0500000004000000080000000042
00790100000078420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000
0000200000000420008010000004042000A07000000044E616D65000000042000B0100000028420055070000000A6172
63686976654B65790000000000042005405000000040000000100000000
```

Out: <empty response payload>

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

```
42007B010000008042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004B751FAC42000D0200000004000000010000000042000F010000002842
005C0500000004000000080000000042007F050000000400000000000000042007C0100000000
```

8

Locate

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

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

Tag: Name Value (0x420055), Type: Text String (0x07), Data: archiveKey
Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007801000000E84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F01000000A042005C05000000040000000800000000420079010000008842008E02000000040000000300000000420008010000002842000A070000000B4F626A6563742054797065000000000042000B05000000040000000200000000420008010000004042000A07000000044E616D650000000042000B0100000028420055070000000A617263686976654B657900000000000042005405000000040000000100000000

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B751FAC42000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F05000000040000000000000042007C0100000030420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000

9

Recover

In: uuidKey, asynchronousIndicator='true'

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

42007801000000A04200770100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000000420007060000000800000000000000142000D0200000004000000010000000042000F010000004842005C050000000400000016000000004200790100000030420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000

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

10

Poll*
In: asynchronousCorrelationValue

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: DDBB075607727F3F

42007801000000704200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000042000D0200000004000000010000000042000F010000002842005C05000000040000001A0000000042007901000000104200060800000008DDBB075607727F3F

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B751FB342000D0200000004000000010000000042000F010000005842005C0500000004000000160000000042007F0500000004000000000000000042007C0100000030420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000

11 Get (symmetric key)
 In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000

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)

42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B751FB342000D0200000004000000010000000042000F01000000C842005C05000000040000000A0000000042007F050000000400000000000000042007C01000000A042005705000000040000000000000420094070000002430643535323136302D666230342D346637632D386137332D666566393035623231633066000000042008F010000005842004001000000504200420500000004000000010000000042004501000000184200430800000010C3200B1291BA648DB9089DED3073DE744200280500000004000000030000000042002A02000000040000008000000000

12

Destroy

In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

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

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000014000000004200790100000030420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000

Out: uuidKey

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FB4 (Fri Feb 12 10:30:28 CET 2010)

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B751FB442000D0200000004000000010000000042000F010000005842005C05000000040000000140000000042007F050000000400000000000000042007C0100000030420094070000002430643535323136302D666230342D346637632D386137332D66656639303562323163306600000000

274
 275
 276
 277
 278
 279
 280
 281
 282
 283
 284
 285
 286
 287
 288
 289
 290
 291

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>Create (symmetric key)</p> <p>In (header): credential={ credentialType='1', credentialValue={ username="Fred", password="password1" } }</p> <p>In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='PolicyKey', NameType='00000001' }, OperationPolicyName='default', CryptographicParameters={ BlockCipherMode='1', PaddingMethod='3', HashingAlgorithm='4' } }</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: Authentication (0x42000C), Type: Structure (0x01), Data:</p> <p> Tag: Credential (0x420023), Type: Structure (0x01), Data:</p> <p> Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password)</p> <p> Tag: Credential Value (0x420025), Type: Structure (0x01), Data:</p> <p> Tag: Username (0x420099), Type: Text String (0x07), Data: Fred</p> <p> Tag: Password (0x4200A1), Type: Text String (0x07), Data: password1</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: Request Payload (0x420079), Type: Structure (0x01), Data:</p> <p> Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)</p> <p> Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:</p>

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)

```
42007801000002504200770100000088420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000C0100000048420023010000004042002405000000040000000100000000420025010000002842
0099070000000446726564000000004200A1070000000970617373776F726431000000000000042000D0200000004000
000010000000042000F01000001B842005C0500000004000000010000000042007901000001A042005705000000040000
0002000000004200910100000188420008010000003042000A070000001743727970746F6772617068696320416C676F7
26974686D0042000B0500000004000000030000000420008010000003042000A070000001443727970746F6772617068
6963204C656E677468000000042000B02000000040000008000000000420008010000003042000A07000000184372797
0746F67726170686963205573616765204D61736B42000B02000000040000000C00000000420008010000004042000A07
000000044E616D650000000042000B01000000284200550700000009506F6C6963794B65790000000000000420054050
00000040000000100000000420008010000003042000A07000000154F7065726174696F6E20506F6C696379204E616D65
00000042000B070000000764656661756C7400420008010000005842000A070000001843727970746F677261706869632
0506172616D657465727342000B01000000304200110500000004000000010000000042005F0500000004000000030000
000042003805000000040000000400000000
```

Out: objectType='00000002', uuidKey

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

- Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 - Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 - Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 - Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 - Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B9F8B4B (Tue Mar 16 14:44:43 CET 2010)
 - Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
- Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 - Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)

Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
 Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000000000004200920900000008000000004B9F8B4B42000D0200000004000000010000000042000F010000006842005C0500000004000000010000000042007F050000000400000000000000042007C01000000404200570500000004000000200000000420094070000002436333437383631352D386236642D346337302D626332332D38643136343831373535356200000000

1 Client A
 Get Attributes, Get
 In (header): credential={ credentialType='1', credentialValue={ username="Fred", password="password1" } }
 In: attributeName='Operation Policy Name'
 In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:
 Tag: Request Header (0x420077), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Authentication (0x42000C), Type: Structure (0x01), Data:
 Tag: Credential (0x420023), Type: Structure (0x01), Data:
 Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password)
 Tag: Credential Value (0x420025), Type: Structure (0x01), Data:
 Tag: Username (0x420099), Type: Text String (0x07), Data: Fred
 Tag: Password (0x4200A1), Type: Text String (0x07), Data: password1
 Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 4CBB6751574C4DA8
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b
 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Operation Policy Name
 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
 Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
 Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 0EA05EE703DA997B
 Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
 Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b

42007801000001704200770100000088420069010000002042006A0200000004000000010000000042006B02000000040000000000000042000C01000000484200230100000040420024050000000400000001000000004200250100000028420099070000000446726564000000004200A1070000000970617373776F72643100000000000042000D02000000040000000000000042000F010000007842005C05000000040000000B0000000042009308000000084CBB6751574C4DA84200790100000050420094070000002436333437383631352D386236642D346337302D626332332D386431363438313735353562000000042000A07000000154F7065726174696F6E20506F6C696379204E616D6500000042000F010000005842005C05000000040000000A0000000042009308000000080EA05EE703DA997B420079010000003042009407000000243633343

7383631352D386236642D346337302D626332332D38643136343831373535356200000000

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)

42007B01000001D842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000042009209000000800000004B9F8B4C42000D020000000400000002000000042000F01000000A042
005C05000000040000000B0000000042009308000000084CBB6751574C4DA842007F050000000400000000000000420
07C0100000068420094070000002436333437383631352D386236642D346337302D626332332D38643136343831373535
356200000000420008010000003042000A07000000154F7065726174696F6E20506F6C696379204E615D650000004200
B07000000764656661756C740042000F01000000D842005C05000000040000000A0000000042009308000000080EA05E
E703DA997B42007F0500000004000000000000000000042007C01000000A0420057050000000400000002000000004200940
70000002436333437383631352D386236642D346337302D626332332D386431363438313735353562000000042008F01
000005842004001000000504200420500000004000000010000000042004501000000184200430800000010C520FCA4E
681F7BFFB3523D71427D5944200280500000004000000030000000042002A02000000040000000800000000

2	Client B
---	----------

Get (symmetric key), Get Attribute List

In (header): credential={ credentialType='1', credentialValue={ username="Barney", password="secret2" } }, BatchOrderOption='true', BatchErrorContinuationOption='Continue'

In: uuidKey

In: uuidKey

Tag: Request Message (0x420078), Type: Structure (0x01), Data:

Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Tag: Authentication (0x42000C), Type: Structure (0x01), Data:

Tag: Credential (0x420023), Type: Structure (0x01), Data:

Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password)

Tag: Credential Value (0x420025), Type: Structure (0x01), Data:

Tag: Username (0x420099), Type: Text String (0x07), Data: Barney

Tag: Password (0x4200A1), Type: Text String (0x07), Data: secret2

Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE

Tag: Batch Error Continuation Option (0x42000E), Type: Enumeration (0x05), Data: 0x00000001

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

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: E3E72D5A352687D8

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

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b

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

Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)

Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: A9A1D60B0C62ECAF

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

Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 63478615-8b6d-4c70-bc23-8d164817555b

420078010000016842007701000000A0420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000C0100000040420023010000003842002405000000040000000100000000420025010000002042
009907000000064261726E657900004200A1070000000773656372657432004200100600000008000000000000001420
00E050000000400000001000000042000D0200000004000000020000000042000F010000005842005C05000000040000
000A00000000420093080000008E3E72D5A352687D84200790100000030420094070000002436333437383631352D386
236642D346337302D626332332D3864313634383137353535620000000042000F010000005842005C0500000004000000
0C000000004200930800000008A9A1D60B0C62ECAF4200790100000030420094070000002436333437383631352D38623
6642D346337302D626332332D38643136343831373535356200000000

Out: Operation Failed, Permission Denied

Out: Operation Failed, Permission Denied

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

Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

```

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

42007B010000011042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004B9F8B4D42000D0200000004000000020000000042000F010000005842
005C05000000040000000A000000004200930800000008E3E72D5A352687D842007F05000000040000000100000000420
07E05000000040000000C0000000042007D070000000D4163636573732064656E696564000000042000F01000000584200
5C05000000040000000C000000004200930800000008A9A1D60B0C62ECAF42007F0500000004000000010000000042007
E05000000040000000C0000000042007D070000000D4163636573732064656E696564000000

```

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
0000000000000042000C0100000048420023010000004042002405000000040000000100000000420025010000002842
009907000000044672656400000004200A1070000000970617373776F72643100000000000042000D0200000004000
000010000000042000F010000004842005C05000000040000001400000000420079010000003042009407000000243633
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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000000400000000000004200920900000008000000004B9F8B4D42000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F050000000400000000000000042007C010000003042009407000000243633437383631352D386236642D346337302D626332332D38643136343831373535356200000000

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

42007801000000F84200770100000088420069010000002042006A0200000004000000010000000042006B02000000004000000000000042000C01000000484200230100000040420024050000000400000001000000004200250100000028420099070000000446726564000000004200A1070000000970617373776F7264310000000000000042000D02000000040000000000000042000F0100000006042005C050000000400000000B00000000420079010000004842009407000000243633437383631352D386236642D346337302D626332332D3864313634383137353535620000000042000A0700000000C44657

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
000000000000004200920900000008000000004B9F8B4E42000D0200000004000000010000000042000F010000008842
005C050000000400000000B0000000042007F050000000400000000000000042007C01000000604200940700000024363
33437383631352D386236642D346337302D626332332D3864313634383137353535620000000042000801000000284200
0A0700000000C44657374726F7920446174650000000042000B0900000008000000004B9F8B4D

292

293

294 12 Query, Maximum Response Size

295

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

297 12.1 Use-case: Query, Maximum Response Size

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

302

Time	Request/Response
0	<p>Query (operations, objects)</p> <p>In (header): maximumResponseSize='256'</p> <p>In: queryFunctions={ '00000001', '00000002' }</p> <p>Tag: Request Message (0x420078), Type: Structure (0x01), Data:</p> <p> Tag: Request Header (0x420077), Type: Structure (0x01), Data:</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: 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)

```
42007801000000904200770100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042005002000000040000001000000000042000D0200000004000000010000000042000F010000003842
005C050000000400000018000000004200790100000020420074050000000400000001000000004200740500000004000
00002000000000
```

Out: Operation Failed, Response Too Large

Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
 Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
 Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
 Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
 Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
 Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B7918AA (Mon Feb 15 10:49:30 CET 2010)
 Tag: 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)

```
42007B01000000C042007A01000000B8420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004B7918AA42007F0500000004000000010000000042007E050000000400
000020000000042007D0700000043526573706F6E73652073697A653A203536382C204D6178696D756D20526573706F6
E73652053697A6520696E6469636174656420696E20726571756573743A2032353600000000042000D02000000040000
000000000000
```

1	<p>Query (operations, objects) In (header): maximumResponseSize='2048' In: queryFunctions={ '00000001', '00000002' }</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: 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:</p>
---	--

Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000001 (Operations)
Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000002 (Objects)

42007801000000904200770100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420050020000000400000800000000042000D0200000004000000010000000042000F010000003842
005C050000000400000018000000004200790100000020420074050000000400000001000000004200740500000004000
000200000000

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
005C0500000004000000180000000042007F0500000004000000000000000042007C01000001B042005C0500000004000
000010000000042005C0500000004000000020000000042005C0500000004000000030000000042005C05000000040000
00040000000042005C0500000004000000080000000042005C0500000004000000090000000042005C050000000400000
00A0000000042005C05000000040000000B0000000042005C05000000040000000C0000000042005C0500000004000000
0D0000000042005C05000000040000000E0000000042005C05000000040000000F0000000042005C05000000040000001
00000000042005C0500000004000000110000000042005C0500000004000000120000000042005C050000000400000013
0000000042005C0500000004000000140000000042005C0500000004000000150000000042005C0500000004000000160
000000042005C0500000004000000180000000042005C0500000004000000190000000042005C05000000040000001A00
0000004200570500000004000000010000000042005705000000040000000200000000420057050000000400000003000
000004200570500000004000000040000000042005705000000040000000600000000

304 A. Acknowledgments

305

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

308 **Original Authors of the initial contribution:**

309 David Babcock, HP
310 Joseph Birr-Pixton, Thales/nCipher
311 Mathias Björkqvist, IBM (editor)
312 John Clark, HP
313 Stan Feather, HP
314 Jon Geater, nCipher
315 Bob Griffin, EMC
316 Robert Haas, IBM
317 Jack Harwood, EMC
318 Vlad Libershteyn, HP
319 Mark Lin, EMC/RSA
320 Brian Metzger, HP
321 Madhav Mutalik, EMC/RSA
322 Anthony Nadalin, IBM
323 René Pawlitzek, IBM (editor)
324 Bruce Rich, IBM
325 Parameswaran Seshan, EMC/RSA
326 John Tattan, EMC

327 **Participants:**

328
329 Mike Allen, PGP Corporation
330 Gordon Arnold, IBM
331 Todd Arnold, IBM
332 Matthew Ball, Oracle Corporation
333 Elaine Barker, NIST
334 Peter Bartok, Venafi, Inc.
335 Mathias Björkqvist, IBM
336 Kevin Bocek, Thales e-Security
337 Kelley Burgin, National Security Agency
338 Jon Callas, PGP Corporation
339 Tom Clifford, Symantec Corp.
340 Graydon Dodson, Lexmark International Inc.
341 Chris Dunn, SafeNet, Inc.
342 Paul Earsy, SafeNet, Inc.
343 Stan Feather, Hewlett-Packard
344 Indra Fitzgerald, Hewlett-Packard
345 Alan Frindell, SafeNet, Inc.
346 Judith Furlong, EMC Corporation
347 Jonathan Geater, Thales e-Security
348 Robert Griffin, EMC Corporation
349 Robert Haas, IBM
350 Thomas Hardjono, M.I.T.
351 Kurt Heberlein, 3PAR, Inc.
352 Marc Hocking, BeCrypt Ltd.
353 Larry Hofer, Emulex Corporation
354 Brandon Hoff, Emulex Corporation
355 Walt Hubis, LSI Corporation

356 Wyllys Ingersoll, Oracle Corporation
 357 Jay Jacobs, Target Corporation
 358 Glen Jaquette, IBM
 359 Scott Kipp, Brocade Communications Systems, Inc.
 360 David Lawson, Emulex Corporation
 361 Hal Lockhart, Oracle Corporation
 362 Robert Lockhart, Thales e-Security
 363 Shyam Mankala, EMC Corporation
 364 Upendra Mardikar, PayPal Inc.
 365 Marc Massar, Individual
 366 Don McAlister, Associate
 367 Hyrum Mills, Mitre Corporation
 368 Bob Nixon, Emulex Corporation
 369 Landon Curt Noll, Cisco Systems, Inc.
 370 René Pawlitzek, IBM
 371 Rob Philpott, EMC Corporation
 372 Scott Rea, Individual
 373 Bruce Rich, IBM
 374 Scott Rotondo, Oracle Corporation
 375 Saikat Saha, Vormetric, Inc.
 376 Anil Saldhana, Red Hat
 377 Subhash Sankuratripati, NetApp
 378 Mark Schiller, Hewlett-Packard
 379 Jitendra Singh, Brocade Communications Systems, Inc.
 380 Servesh Singh, EMC Corporation
 381 Terence Spies, Voltage Security
 382 Sandy Stewart, Oracle Corporation
 383 Marcus Streets, Thales e-Security
 384 Brett Thompson, SafeNet, Inc.
 385 Benjamin Tomhave, Individual
 386 Sean Turner, IECA, Inc.
 387 Paul Turner, Venafi, Inc.
 388 Marko Vukolić, IBM
 389 Rod Wideman, Quantum Corporation
 390 Steven Wierenga, Hewlett-Packard
 391 Peter Yee, EMC Corporation
 392 Krishna Yellepeddy, IBM
 393 Peter Zelechowski, Election Systems & Software
 394 Grace Zhang, Skyworth TTG Holdings Limited

395 B. Revision History

Revision	Date	Editor	Changes Made
ed-0.98	2009-04-28	Mathias Björkqvist	Initial conversion of input document to OASIS format.
ed-0.98	2009-08-06	Mathias Björkqvist	Changes to layout and message content to reflect the recent changes to the KMIP specification, added descriptions to the use-cases for which they were missing.
ed-0.98	2009-09-28	Mathias Björkqvist	Updated messages and TTLV encodings to conform with KMIP specification ed-0.98 rev 17.
draft-01	2009-10-08	Mathias Björkqvist	Removed normative words “must”, “shall”, “required”, “will” and “can”; updated messages and TTLV encodings to conform to KMIP specification ed-0.98 rev 19; added

			normative references; added minor edits
draft-02	2009-10-15	Mathias Björkqvist	Replaced the TBDs, changed status to Committee Draft, changed use-cases to use protocol major version 1 and minor version 0
draft-03	2009-10-15	Mathias Björkqvist	Corrected names of TC chairs
draft-04	2009-11-05	Mathias Björkqvist	Added list of participants, added reference to Profiles document, line spacing change to list of original contributors, added related documents
cd-05	2009-11-06	Mathias Björkqvist	Changes to various naming aspects on front page and document footer. This is the tentative version for public review.
cd-06	2009-11-12	Mathias Björkqvist	Updated tags.
cd-07	2010-02-17	Mathias Björkqvist	Addressed public review comments, added line numbering.
cd-08	2010-03-17	Mathias Björkqvist	Registration of Templates changed to use the Template object, Usage Allocation changes (Add Attribute, Check, Get Usage Allocation), batched Revoke requests with Destroy requests when destroying objects in the Active state, adopted new format for Username and Password Credential object.
cd-09	2010-03-18	Mathias Björkqvist	Updated participants' list. Editorial fixes.

396