



TBD (Key Management Interoperability Protocol Use Cases)

Editor's Draft 0.98

28 April 2009

Specification URIs:

This Version:

[TBD.html](#)
[TBD.doc](#) (Authoritative)
[TBD.pdf](#)

Previous Version:

[TBD.html](#)
[TBD.doc](#) (Authoritative)
[TBD.pdf](#)

Latest Version:

[TBD.html](#)
[TBD.doc](#)
[TBD.pdf](#)

Technical Committee:

[OASIS Key Management Interoperability Protocol \(KMIP\) TC](#)

Chair(s):

Robert Griffin
Anthony Nadalin

Editor(s):

Robert Haas

Related work:

This specification replaces or supersedes:

- None

This specification is related to:

- TBD

Declared XML Namespace(s):

TBD

Abstract:

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

Status:

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

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the

“Send A Comment” button on the Technical Committee’s web page at <http://www.oasis-open.org/committees/kmip/>.

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

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

Notices

Copyright © OASIS® 2009. All Rights Reserved.

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

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

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

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

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

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

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

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

Table of Contents

1 Introduction	5
1.1 Document Roadmap	5
1.2 Goals and Requirements.....	5
1.3 Notational Conventions	5
1.4 Namespaces	5
1.5 Terminology	5
1.6 Normative References.....	5
1.7 Non-normative References	5
1.8 Compliance	5
2 Message exchange	5
3 Centralized Management	5
3.1 Basic functionality	5
3.1.1 Use-case: Create / Destroy	6
3.1.2 Use-case: Register / Create / Get attributes / Destroy	8
3.1.3 Use-case: Create / Locate / Get / Destroy.....	13
3.1.4 Use-case: Dual client use-case, ID Placeholder linked Locate & Get batch.....	18
3.2 Use-case: Asynchronous Locate.....	32
4 Key life cycle support.....	42
4.1 Use-case: Revoke scenario	42
5 Auditing and reporting	59
5.1 Use-case: Get usage allocation scenario	59
6 Key Interchange, Key Exchange	71
6.1 Use-case: Import of a Third-party Key.....	71
7 Vendor Extensions	74
7.1 Use-case: Unrecognized Message Extension with Criticality Indicator false	74
7.2 Use-case: Unrecognized Message Extension with Criticality Indicator true.....	75
8 Asymmetric keys	75
8.1 Use-case: Create a Key Pair.....	75
8.2 Use-case: Register Both Halves of a Key Pair	76
9 Key Roll-over.....	77
9.1 Use-case: Create a Key, Re-key	77
9.2 Use-case: Existing Key Expired, Re-key with Same lifecycle	78
9.3 Use-case: Existing Key Compromised, Re-key with same lifecycle.....	79
9.4 Use-case: Create key, Re-key with new lifecycle	80
9.5 Use-case: Obtain Lease for Expired Key.....	81
10 Archival	82
10.1 Use-case: Create a Key, Archive and Recover it.....	82
A. Acknowledgments.....	84
B. Revision History	85

1 Introduction

The purpose of this document is to describe use-cases to demonstrate the Key Management Interoperability Protocol (KMIP). The use-cases shall indicate if all concepts within the protocol are sound and can be used to implement typical scenarios in real life. These use-cases are not intended to fully test an implementation of KMIP. Thus, the use-cases do not contain typical QA scenarios which would stress an implementation. The use-cases are based on v0.98 of the protocol.

1.1 Document Roadmap

[TBD](#)

1.2 Goals and Requirements

[TBD](#)

1.3 Notational Conventions

[TBD](#)

1.4 Namespaces

[TBD](#)

1.5 Terminology

[TBD](#)

1.6 Normative References

[TBD](#)

1.7 Non-normative References

[TBD](#)

1.8 Compliance

[TBD](#)

2 Message exchange

The message exchange between clients and the server to test the following use-case scenarios shall happen with TLV encoding over the http transport.

3 Centralized Management

3.1 Basic functionality

This use-case tests the basic features of KMIP including key and template creation, attribute functionality, access methods, and batch operation.

3.1.1 Use-case: Create / Destroy

Time	Request/Response messages
0	<p>Create (symmetric key)</p> <p>In: objectType='00000002' (Symmetric Key), CryptographicAlgorithm='00000003' (AES), CryptographicLength='128', CryptographicUsageMask='00000012'</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data:</p> <ul style="list-style-type: none"> Tag: Request Header (0x42000072), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98) Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1) Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000001 (Create) Tag: Request Payload (0x42000074), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x4200008D), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Attribute (0x42000008), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Algorithm Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000003 (AES) Tag: Attribute (0x42000008), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Length Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x00000080 (128) Tag: Attribute (0x42000008), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Usage Mask Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x0000000C (Encrypt, Decrypt) <p>42000073800000010E42000072800000003042000065800000001A4200006601000000040000000042000067010000000400000062420000D01000000400000001420000F80000000CC42000057040000000400000014200007480000000B6420000520400000004000000024200008D80000000A042000008800000002D4200000A060000001743727970746F6772617068696320416C676F726974686D4200000B040000004000000034200008800000002A4200000A060000001443727970746F67726170686963204C656E6774684200000B010000000400000008042000008800000002E4200000A060000001843727970746F67726170686963205573616765204D61736B4200000B0100000040000000C</p> <p>Out: objectType='00000002', uuidKey</p> <p>Tag: Response Message (0x42000076), Type: Structure (0x80), Data:</p> <ul style="list-style-type: none"> Tag: Response Header (0x42000075), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98) Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496DFEDC (Wed Jan 14

16:03:56 CET 2009)

- Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
- Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 - Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000001 (Create)
 - Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 - Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 - Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
 - Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 96789141-62bf-4352-blc4-9d48dac4b77d

4200007680000000B042000075800000004142000065800000001A42000066010000000400000000420000670100000004000000624200008E080000000800000000496DFEDC420000D0100000004000000014200000F800000005D42000057040000004000000014200007A0400000004000000042000077800000003A42000052040000004000000024200008F060000002439363738393134312D363262662D343335322D623163342D396434386461633462373764

1

Destroy (symmetric key)
In: uuidKey

- Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 - Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 - Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 - Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 - Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 - Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 - Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 - Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy)
 - Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 - Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 96789141-62bf-4352-blc4-9d48dac4b77d

42000073800000008542000072800000003042000065800000001A4200006601000000040000000042000067010000000400000062420000D0100000004000000014200000F80000000434200005704000000040000001442000074800000002D4200008F0600000002439363738393134312D363262662D343335322D623163342D396434386461633462373764

Out: uuidKey

- Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 - Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 - Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 - Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 - Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 - Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496DFEDD (Wed Jan 14 16:03:57 CET 2009)
 - Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 - Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 - Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy)
 - Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 - Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 - Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 96789141-62bf-4352-blc4-9d48dac4b77d

```

4200007680000000A342000075800000004142000065800000001A420000660100000004000000004200006701000000
04000000624200008E080000000800000000496DFEDD4200000D0100000004000000014200000F800000005042000057
0400000004000000144200007A0400000004000000042000077800000002D4200008F06000000243936373839313431
2D363262662D343335322D623163342D396434386461633462373764

```

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

Time	Request/Response messages
0	<p>Register (template)</p> <p>In: objectType='00000007', templateName = 'Template1', attributes={ ObjectGroup='Group1', ApplicationSpecificID='ssl, www.example.com', ContactInformation='Joe', x-Purpose='demonstration' }</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data:</p> <p> Tag: Request Header (0x42000072), Type: Structure (0x80), Data:</p> <p> Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:</p> <p> Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)</p> <p> Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)</p> <p> Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)</p> <p> Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:</p> <p> Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000003 (Register)</p> <p> Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:</p> <p> Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000006 (Template)</p> <p> Tag: Template Name (0x4200008C), Type: Text String (0x06), Data: Template1</p> <p> Tag: Template-Attribute (0x4200008D), Type: Structure (0x80), Data:</p> <p> Tag: Attribute (0x42000008), Type: Structure (0x80), Data:</p> <p> Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Group</p> <p> Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Group1</p> <p> Tag: Attribute (0x42000008), Type: Structure (0x80), Data:</p> <p> Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Application Specific Identification</p> <p> Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:</p> <p> Tag: Application Name Space (0x42000003), Type: Text String (0x06), Data: ssl</p> <p> Tag: Application Identifier (0x42000002), Type: Text String (0x06), Data: www.example.com</p> <p> Tag: Attribute (0x42000008), Type: Structure (0x80), Data:</p> <p> Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Contact Information</p> <p> Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Joe</p> <p> Tag: Attribute (0x42000008), Type: Structure (0x80), Data:</p> <p> Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-Purpose</p> <p> Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: demonstration</p> <p>42000073800000017142000072800000003042000065800000001A420000660100000004000000004200006701000000 4000000624200000D0100000004000000014200000F800000012F42000057040000000400000003420000748000000119 420000520400000004000000064200008C060000000954656D706C617465314200008D80000000F142000008800000002 44200000A060000000C4F626A6563742047726F75704200000B060000000647726F757031420000088000000059420000 0A06000000234170706C69636174696F6E205370656369666963204964656E74696669636174696F6E4200000B8000000 02442000003060000000373736C42000002060000000F7777772E6578616D706C652E636F6D4200000880000000284200</p>

000A0600000013436F6E7461637420496E666F726D6174696F6E420000B0600000034A6F654200008800000028420
0000A0600000009782D507572706F7365420000B06000000D64656D6F6E7374726174696F6E

Out: objectType='0000007', uuidTemplate

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496DFEDE (Wed Jan 14
16:03:58 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000003 (Register)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000006 (Template)
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 14856cce-fc2a-499b-
9f2d-5c6924838b1f

4200007680000000B042000075800000004142000065800000001A42000066010000000400000004200006701000000
4000000624200008E080000000800000000496DFEDE420000D010000000400000001420000F800000005D4200005704
00000004000000034200007A04000000040000000042000077800000003A420000520400000004000000064200008F060
000002431343835366363652D666332612D343939622D396632642D356336393234383338623166

1

Create (symmetric key using template)

In: objectType='0000002', templateName='Template1', CryptographicAlgorithm='AES',
CryptographicLength='128', CryptographicUsageMask='00000012'

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000001 (Create)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
 Tag: Template-Attribute (0x4200008D), Type: Structure (0x80), Data:
 Tag: Template Name (0x4200008C), Type: Text String (0x06), Data: Template1
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic
Algorithm
 Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000003 (AES)
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Length
 Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x00000080 (128)
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Usage

	<p>Mask</p> <p>Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x0000000C (Encrypt, Decrypt)</p> <p>42000073800000012042000072800000003042000065800000001A42000066010000000400000000420000670100000004000000624200000D0100000004000000014200000F80000000DE420000570400000004000000014200007480000000C8420000520400000004000000024200008D80000000B24200008C060000000954656D706C6174653142000008800000002D4200000A060000001743727970746F6772617068696320416C676F726974686D4200000B0400000004000000034200000880000002A4200000A060000001443727970746F67726170686963204C656E6774684200000B01000000040000000804200000880000002E4200000A060000001843727970746F67726170686963205573616765204D61736B4200000B01000000400000000C</p> <p>Out: objectType='00000002', uuidKey</p> <p>Tag: Response Message (0x42000076), Type: Structure (0x80), Data:</p> <p>Tag: Response Header (0x42000075), Type: Structure (0x80), Data:</p> <p>Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:</p> <p>Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)</p> <p>Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)</p> <p>Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496DFEDF (Wed Jan 14 16:03:59 CET 2009)</p> <p>Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:</p> <p>Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000001 (Create)</p> <p>Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)</p> <p>Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:</p> <p>Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)</p> <p>Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6f2bb284-0488-4d4f-b0a2-ela9cb33b33f</p> <p>4200007680000000B042000075800000004142000065800000001A42000066010000000400000000420000670100000004000000624200008E080000000800000000496DFEDF4200000D0100000004000000014200000F800000005D420000570400000004000000014200007A04000000040000000042000077800000003A420000520400000004000000024200008F060000002436663262623238342D303438382D346434662D623061322D653161396362333362333366</p>
2	<p>Get attributes</p> <p>In: uuidKey, attributeNames={'ObjectGroup', 'ApplicationSpecificID', 'ContactInformation', 'x-Purpose'}</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data:</p> <p>Tag: Request Header (0x42000072), Type: Structure (0x80), Data:</p> <p>Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:</p> <p>Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)</p> <p>Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)</p> <p>Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:</p> <p>Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000B (Get Attributes)</p> <p>Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:</p> <p>Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6f2bb284-0488-4d4f-b0a2-ela9cb33b33f</p> <p>Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Group</p> <p>Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Application Specific Identification</p> <p>Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Contact Information</p>

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-Purpose

4200007380000000F442000072800000003042000065800000001A4200006601000000040000000042000067010000000
4000000624200000D0100000004000000014200000F80000000B24200005704000000040000000B42000074800000009C
4200008F060000002436663262623238342D303438382D346434662D623061322D6531613963623333664200000
A060000000C4F626A6563742047726F75704200000A06000000234170706C69636174696F6E2053706563696669632049
64656E74696669636174696F6E4200000A0600000013436F6E7461637420496E666F726D6174696F6E4200000A0600000
009782D507572706F7365

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

Tag: Response Header (0x42000075), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496DFEDF (Wed Jan 14 16:03:59 CET 2009)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000B (Get Attributes)

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)

Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6f2bb284-0488-4d4f-b0a2-ela9cb33b33f

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Group

Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Group1

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Application Specific Identification

Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:

Tag: Application Name Space (0x42000003), Type: Text String (0x06), Data: ssl

Tag: Application Identifier (0x42000002), Type: Text String (0x06), Data: www.example.com

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Contact Information

Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Joe

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-Purpose

Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: demonstration

4200007680000000194420000758000000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496DFEDF420000D010000000400000001420000F80000001414200005704
0000000400000000B4200007A04000000040000000042000077800000011E4200008F060000002436663262623238342D3
03438382D346434662D623061322D65316139636233362333366420000880000000244200000A060000000C4F626A65
63742047726F75704200000B060000000647726F757031420000880000000594200000A060000000234170706C6963617
4696F6E205370656369666963204964656E74696669636174696F6E4200000B800000002442000003060000000373736C
42000002060000000F777772E6578616D706C652E636F6D4200000880000000284200000A0600000013436F6E7461637
420496E666F726D6174696F6E4200000B06000000034A6F65420000880000000284200000A0600000009782D50757270
6F73654200000B060000000D64656D6F6E7374726174696F6E

3 Destroy (symmetric key)

In: uuidKey

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy)
Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6f2bb284-0488-4d4f-b0a2-ela9cb33b33f

42000073800000008542000072800000003042000065800000001A4200006601000000040000000042000067010000000
4000000624200000D0100000004000000014200000F80000000434200005704000000040000001442000074800000002D
4200008F060000002436663262623238342D303438382D346434662D623061322D653161396362333362333366

Out: uuidKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496DFEDF (Wed Jan 14 16:03:59 CET 2009)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy)
Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6f2bb284-0488-4d4f-b0a2-ela9cb33b33f

4200007680000000A3420000758000000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496DFEDF4200000D0100000004000000014200000F80000000504200005704
00000004000000144200007A04000000040000000042000077800000002D4200008F060000002436663262623238342D3
03438382D346434662D623061322D653161396362333362333366

4

Destroy (template)
In: uuidTemplate

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy)

	<p>Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:</p> <p>Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 14856cce-fc2a-499b-9f2d-5c6924838blf</p> <p>42000073800000008542000072800000003042000065800000001A42000066010000000400000000420000670100000004000000624200000D01000000004000000014200000F800000004342000057040000000400000014420000748000000002D4200008F060000002431343835366363652D666332612D343939622D396632642D356336393234383338623166</p> <p>Out: uuidTemplate</p> <p>Tag: Response Message (0x42000076), Type: Structure (0x80), Data:</p> <p>Tag: Response Header (0x42000075), Type: Structure (0x80), Data:</p> <p>Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:</p> <p>Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)</p> <p>Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)</p> <p>Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496DFEE0 (Wed Jan 14 16:04:00 CET 2009)</p> <p>Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:</p> <p>Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy)</p> <p>Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)</p> <p>Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:</p> <p>Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 14856cce-fc2a-499b-9f2d-5c6924838blf</p> <p>4200007680000000A342000075800000004142000065800000001A42000066010000000400000000420000670100000004000000624200008E0800000000800000000496DFEE04200000D0100000004000000014200000F8000000050420000570400000004000000144200007A04000000040000000042000077800000002D4200008F060000002431343835366363652D666332612D343939622D396632642D356336393234383338623166</p>
--	---

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

Time	Request/Response messages
0	<p>Create (symmetric key)</p> <p>In: objectType = '00000002', attributes={ Name={ Name='Key1', NameType='00000001' }, CryptographicAlgorithm='DES', CryptographicLength='56', CryptographicUsageMask='00000012', ContactInformation='Joe' }</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data:</p> <p>Tag: Request Header (0x42000072), Type: Structure (0x80), Data:</p> <p>Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:</p> <p>Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)</p> <p>Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)</p> <p>Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:</p> <p>Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000001 (Create)</p> <p>Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:</p>

Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
Tag: Template-Attribute (0x4200008D), Type: Structure (0x80), Data:
Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name
Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:
Tag: Name Value (0x42000050), Type: Text String (0x06), Data: Key1
Tag: Name Type (0x4200004F), Type: Enumeration (0x04), Data: 0x00000001
(Uninterpreted text string)

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic
Algorithm
Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000001 (DES)
Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Length
Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x00000038 (56)

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Usage
Mask
Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x0000000C (Encrypt,
Decrypt)

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Contact Information
Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Joe

42000073800000017842000072800000003042000065800000001A420000660100000004000000042000067010000000
40000062420000D0100000040000001420000F800000013642000570400000040000001420000748000000120
42000052040000000400000024200008D800000010A42000008800000030420000A06000000044E616D654200000B8
00000001A4200005006000000044B6579314200004F040000000400000014200008800000002D420000A0600000017
43727970746F6772617068696320416C676F726974686D4200000B040000000400000014200008800000002A4200000
A060000001443727970746F67726170686963204C656E6774684200000B0100000004000000384200008800000002E42
0000A060000001843727970746F67726170686963205573616765204D61736B4200000B01000000040000000C4200000
88000000028420000A0600000013436F6E7461637420496E666F726D6174696F6E4200000B06000000034A6F65

Out: objectType = '00000002', uuidKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E00BB (Wed Jan 14
16:11:55 CET 2009)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000001 (Create)
Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 579639a1-798e-4b0a-
ba4f-e16c5cb2c18c

4200007680000000B042000075800000004142000065800000001A420000660100000004000000042000067010000000
400000624200008E08000000080000000496E00BB420000D0100000040000001420000F800000005D4200005704

00000004000000014200007A04000000040000000042000077800000003A420000520400000004000000024200008F060000002435373936333961312D373938652D346230612D626134662D653136633563623263313863

1

Locate (symmetric key)

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:

Tag: Request Header (0x42000072), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)

Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Type

Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric

Key)

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name

Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:

Tag: Name Value (0x42000050), Type: Text String (0x06), Data: Key1

Tag: Name Type (0x4200004F), Type: Enumeration (0x04), Data: 0x00000001 (Uninterpreted text string)

4200007380000000BB42000072800000003042000065800000001A420000660100000004000000042000067010000000400000062420000D010000000400000001420000F800000007942000057040000000400000008420000748000000063420000880000000021420000A060000000B4F626A65637420547970654200000B04000000040000000242000088000000030420000A06000000044E616D65420000B800000001A4200005006000000044B6579314200004F040000000400000001

Out: uuidKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

Tag: Response Header (0x42000075), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E00BB (Wed Jan 14 16:11:55 CET 2009)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)

Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 579639a1-798e-4b0a-ba4f-e16c5cb2c18c

4200007680000000A342000075800000004142000065800000001A4200006601000000040000000420000670100000004000000624200008E080000000800000000496E00BB420000D010000000400000001420000F8000000050420000570400000004000000084200007A04000000040000000042000077800000002D4200008F0600000002435373936333961312D3

73938652D346230612D626134662D653136633563623263313863

2

Get (symmetric key)

In: uuidKey

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:

Tag: Request Header (0x42000072), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)

Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 579639a1-798e-4b0a-ba4f-e16c5cb2c18c

42000073800000008542000072800000003042000065800000001A4200006601000000040000000042000067010000000
4000000624200000D0100000004000000014200000F80000000434200005704000000040000000A42000074800000002D
4200008F060000002435373936333961312D373938652D346230612D626134662D653136633563623263313863

Out: objectType = '00000002', uuidKey, symmetricKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

Tag: Response Header (0x42000075), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E00BC (Wed Jan 14 16:11:56 CET 2009)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)

Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 579639a1-798e-4b0a-ba4f-e16c5cb2c18c

Tag: Symmetric Key (0x4200008A), Type: Structure (0x80), Data:

Tag: Key Block (0x4200003C), Type: Structure (0x80), Data:

Tag: Key Value Type (0x42000040), Type: Enumeration (0x04), Data: 0x00000001

Tag: Key Value (0x4200003F), Type: Structure (0x80), Data:

Tag: Key Material (0x4200003D), Type: Octet String (0x07), Data: FDE6BF0BE59D9D4F

Tag: Cryptographic Algorithm (0x42000025), Type: Enumeration (0x04), Data: 0x00000001 (DES)

Tag: Cryptographic Length (0x42000026), Type: Integer (0x01), Data: 0x00000038 (56)

42000076800000010342000075800000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E00BC420000D0100000004000000014200000F80000000B04200005704
000000040000000A4200007A04000000040000000042000077800000008D420000520400000004000000024200008F060
000002435373936333961312D373938652D346230612D626134662D6531366335636232633138634200008A800000004A
4200003C8000000041420000400400000004000000014200003F80000000114200003D0700000008FDE6BF0BE59D9D4F4

	200002504000000040000000142000026010000000400000038
3	<p>Destroy (symmetric key) In: uuidKey</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data: Tag: Request Header (0x42000072), Type: Structure (0x80), Data: Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98) Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1) Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data: Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy) Tag: Request Payload (0x42000074), Type: Structure (0x80), Data: Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 579639a1-798e-4b0a-ba4f-e16c5cb2c18c</p> <p>42000073800000008542000072800000003042000065800000001A4200006601000000040000000042000067010000000 4000000624200000D0100000004000000014200000F80000000434200005704000000040000001442000074800000002D 4200008F060000002435373936333961312D373938652D346230612D626134662D653136633563623263313863</p> <p>Out: uuidKey</p> <p>Tag: Response Message (0x42000076), Type: Structure (0x80), Data: Tag: Response Header (0x42000075), Type: Structure (0x80), Data: Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98) Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E00BC (Wed Jan 14 16:11:56 CET 2009) Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1) Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data: Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy) Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success) Tag: Response Payload (0x42000077), Type: Structure (0x80), Data: Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 579639a1-798e-4b0a-ba4f-e16c5cb2c18c</p> <p>42000076800000000A342000075800000004142000065800000001A4200006601000000040000000042000067010000000 4000000624200008E080000000800000000496E00BC4200000D0100000004000000014200000F80000000504200005704 00000004000000144200007A04000000040000000042000077800000002D4200008F060000002435373936333961312D3 73938652D346230612D626134662D653136633563623263313863</p>
4	<p>Locate In: uuidKey</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data: Tag: Request Header (0x42000072), Type: Structure (0x80), Data: Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)</p>

```

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
  Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)
  Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
    Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
      Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Unique Identifier
      Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: 579639a1-798e-4b0a-
ba4f-e16c5cb2c18c

4200007380000000A842000072800000003042000065800000001A4200006601000000040000000042000067010000000
4000000624200000D0100000004000000014200000F800000006642000057040000000400000008420000748000000050
4200000880000000474200000A0600000011556E69717565204964656E74696666965724200000B0600000024353739363
33961312D373938652D346230612D626134662D653136633563623263313863

Out: <empty response payload>

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
  Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
    Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
      Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
    Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E00BC (Wed Jan 14
16:11:56 CET 2009)
    Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
    Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
      Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)
      Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
      Tag: Response Payload (0x42000077), Type: Structure (0x80), Data: null

42000076800000007642000075800000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E00BC4200000D0100000004000000014200000F800000000234200005704
00000004000000084200007A040000000400000000420000778000000000

```

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

Time	Request/Response messages
0	<p>Client A:</p> <p>Register (template)</p> <p>In: objectType='00000007', templateName = 'Template1', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128' }</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data:</p> <p>Tag: Request Header (0x42000072), Type: Structure (0x80), Data:</p> <p>Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:</p> <p>Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)</p>

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000003 (Register)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000006 (Template)
 Tag: Template Name (0x4200008C), Type: Text String (0x06), Data: Template1
 Tag: Template-Attribute (0x4200008D), Type: Structure (0x80), Data:
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic
 Algorithm
 Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000003 (AES)
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Length
 Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x00000080 (128)

4200007380000000E942000072800000003042000065800000001A420000660100000004000000004200006701000000
 40000062420000D010000000400000001420000F80000000A74200005704000000040000000342000074800000091
 420000520400000004000000064200008C060000000954656D706C617465314200008D80000000694200008800000002
 D4200000A060000001743727970746F6772617068696320416C676F726974686D4200000B040000000400000003420000
 08800000002A420000A060000001443727970746F67726170686963204C656E6774684200000B010000000400000080

Out: objectType='00000007', uuidTemplate

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E01CF (Wed Jan 14
 16:16:31 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000003 (Register)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000006 (Template)
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 7936e2b9-0185-43ab-
 81b1-2e644ae48996

4200007680000000B042000075800000004142000065800000001A420000660100000004000000004200006701000000
 400000624200008E08000000080000000496E01CF420000D010000000400000001420000F800000005D4200005704
 00000004000000034200007A04000000040000000042000077800000003A420000520400000004000000064200008F060
 000002437393336653262392D303138352D343361622D383162312D326536343461653438393936

1

Client A:

Create (symmetric key using template)

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:

```

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
  Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
  Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
  Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000001 (Create)
  Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
    Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
    Tag: Template-Attribute (0x4200008D), Type: Structure (0x80), Data:
      Tag: Template Name (0x4200008C), Type: Text String (0x06), Data: Template1
      Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
        Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name
        Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:
          Tag: Name Value (0x42000050), Type: Text String (0x06), Data: Key1
          Tag: Name Type (0x4200004F), Type: Enumeration (0x04), Data: 0x00000001
(Uninterpreted text string)
        Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
          Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x00000004 (Encrypt)
        Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
          Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Contact Information
          Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Foo

```

```

42000073800000012142000072800000003042000065800000001A420000660100000004000000004200006701000000
4000000624200000D0100000004000000014200000F80000000DF420000570400000004000000014200007480000000C9
420000520400000004000000024200008D80000000B34200008C060000000954656D706C6174653142000008800000003
04200000A06000000044E616D654200000B800000001A4200005006000000044B6579314200004F040000000400000001
42000008800000002E4200000A060000001843727970746F67726170686963205573616765204D61736B4200000B01000
000040000000044200000880000000284200000A0600000013436F6E7461637420496E666F726D6174696F6E4200000B06
00000003466F6F

```

Out: objectType='00000002', uuidKey

```

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
  Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
    Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
      Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
    Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E01D0 (Wed Jan 14
16:16:32 CET 2009)
    Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
  Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
    Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000001 (Create)
    Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
      Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-
9ad8-0cff0bcbe9c1

```

```

4200007680000000B042000075800000004142000065800000001A420000660100000004000000004200006701000000
4000000624200008E08000000080000000496E01D0420000D0100000004000000014200000F800000005D4200005704
00000004000000014200007A04000000040000000042000077800000003A420000520400000004000000024200008F060

```

000002461646264656638642D643662632D343838612D396164382D306366663062636265396331

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 (0x42000073), Type: Structure (0x80), Data:

Tag: Request Header (0x42000072), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Batch Order Option (0x42000010), Type: Boolean (0x05), Data: TRUE

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)

Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 1FADF4F046275B0E

Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Type

Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric

Key)

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name

Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:

Tag: Name Value (0x42000050), Type: Text String (0x06), Data: Key1

Tag: Name Type (0x4200004F), Type: Enumeration (0x04), Data: 0x00000001 (Uninterpreted text string)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)

Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: FDBE797C64556C51

Tag: Request Payload (0x42000074), Type: Structure (0x80), Data: null

42000073800000010642000072800000003A42000065800000001A4200006601000000040000000042000067010000000
400000062420000100500000001014200000D0100000004000000024200000F800000008A420000570400000004000000
084200009007000000081FADF4F046275B0E42000074800000000634200000880000000214200000A060000000B4F626A6
5637420547970654200000B0400000004000000024200000880000000304200000A06000000044E616D654200000B8000
00001A4200005006000000044B6579314200004F0400000004000000014200000F8000000027420000570400000004000
0000A420000900700000008FDBE797C64556C51420000748000000000

Out: uuidKey

Out: objectType='00000002', uuidKey, symmetricKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

Tag: Response Header (0x42000075), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E01D1 (Wed Jan 14

```

16:16:33 CET 2009)
  Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)
  Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
    Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)
    Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 1FADF4F046275B0E
    Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
      Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1
    Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
      Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
      Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: FDBE797C64556C51
      Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
      Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
        Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
        Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1
        Tag: Symmetric Key (0x4200008A), Type: Structure (0x80), Data:
          Tag: Key Block (0x4200003C), Type: Structure (0x80), Data:
            Tag: Key Value Type (0x42000040), Type: Enumeration (0x04), Data: 0x00000001
            Tag: Key Value (0x4200003F), Type: Structure (0x80), Data:
              Tag: Key Material (0x4200003D), Type: Octet String (0x07), Data:
200003F80000000194200003D07000000105C6BB5838B5E8DF9AC4B6D9F3913175E
              Tag: Cryptographic Algorithm (0x42000025), Type: Enumeration (0x04), Data: 0x00000003
(AES)
              Tag: Cryptographic Length (0x42000026), Type: Integer (0x01), Data: 0x00000080 (128)

42000076800000018642000075800000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E01D14200000D0100000004000000024200000F800000000614200005704
00000004000000084200009007000000081FADF4F046275B0E4200007A04000000040000000042000077800000002D420
0008F060000002461646264656638642D643662632D343838612D396164382D306366663062636265396331420000F80
000000C94200005704000000040000000A420000900700000008FDBE797C64556C514200007A040000000400000000420
000778000000095420000520400000004000000024200008F060000002461646264656638642D643662632D343838612D
396164382D3063666630626362653963314200008A80000000524200003C8000000049420000400400000004000000014
200003F80000000194200003D07000000105C6BB5838B5E8DF9AC4B6D9F3913175E420000250400000004000000034200
0026010000000400000080

```

3	<p>Client B: Get attribute list In: uuidKey</p> <pre> Tag: Request Message (0x42000073), Type: Structure (0x80), Data: Tag: Request Header (0x42000072), Type: Structure (0x80), Data: Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98) Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1) Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data: Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000C (Get Attribute List) Tag: Request Payload (0x42000074), Type: Structure (0x80), Data: Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1 </pre>
---	---

4200007380000008542000072800000003042000065800000001A4200006601000000040000000042000067010000000
4000000624200000D0100000004000000014200000F80000000434200005704000000040000000C42000074800000002D
4200008F060000002461646264656638642D643662632D343838612D396164382D306366663062636265396331

Out: uuidKey, attributes={ * }

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

Tag: Response Header (0x42000075), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E01D1 (Wed Jan 14 16:16:33 CET 2009)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000C (Get Attribute List)

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)

Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Length

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Algorithm

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: State

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Initial Date

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Unique Identifier

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Usage Mask

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Type

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Contact Information

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Last Changed Date

42000076800000019542000075800000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E01D14200000D0100000004000000014200000F80000001424200005704
000000040000000C4200007A04000000040000000042000077800000011F4200008F060000002461646264656638642D6
43662632D343838612D396164382D3063666630626362653963314200000A060000001443727970746F67726170686963
204C656E6774684200000A060000001743727970746F6772617068696320416C676F726974686D4200000A06000000055
3746174654200000A060000000C496E697469616C20446174654200000A0600000011556E69717565204964656E746966
6965724200000A06000000044E616D654200000A060000001843727970746F67726170686963205573616765204D61736
B4200000A060000000B4F626A65637420547970654200000A0600000013436F6E7461637420496E666F726D6174696F6E
4200000A06000000114C617374204368616E6765642044617465

4

Client B:

Get attributes

In: uuidKey, attributeNames={'Name', 'ContactInformation'}

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:

Tag: Request Header (0x42000072), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000B (Get Attributes)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Contact Information

4200007380000000AE42000072800000003042000065800000001A4200006601000000040000000042000067010000000
 4000000624200000D0100000004000000014200000F800000006C4200005704000000040000000B420000748000000056
 4200008F060000002461646264656638642D643662632D343838612D396164382D3063666630626362653963314200000
 A06000000044E616D654200000A0600000013436F6E7461637420496E666F726D6174696F6E

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E01D2 (Wed Jan 14 16:16:34 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000B (Get Attributes)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name
 Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:
 Tag: Name Value (0x42000050), Type: Text String (0x06), Data: Key1
 Tag: Name Type (0x4200004F), Type: Enumeration (0x04), Data: 0x00000001 (Uninterpreted text string)
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Contact Information
 Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Foo

42000076800000010D42000075800000004142000065800000001A4200006601000000040000000042000067010000000
 4000000624200008E080000000800000000496E01D2420000D0100000004000000014200000F80000000BA4200005704
 000000040000000B4200007A0400000004000000004200007780000000974200008F060000002461646264656638642D6
 43662632D343838612D396164382D3063666630626362653963314200000880000000304200000A06000000044E616D65
 4200000B800000001A4200005006000000044B6579314200004F0400000004000000014200000880000000284200000A0
 600000013436F6E7461637420496E666F726D6174696F6E4200000B0600000003466F6F

5	<p>Client B: Add attribute [batch] In: uuidKey, attribute={ x-attribute1='Value1' } In: uuidKey, attribute={ x-attribute2='Value2' }</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data: Tag: Request Header (0x42000072), Type: Structure (0x80), Data:</p>
---	--

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

- Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
- Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

- Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)
- Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 208BA9C5EFCAA530
- Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:

 - Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

- Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute1
- Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Value1

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

- Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)
- Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: A3E3990370185C0A
- Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:

 - Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

- Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute2
- Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Value2

42000073800000014D42000072800000003042000065800000001A420000660100000004000000042000067010000000
4000000624200000D0100000004000000024200000F80000000814200005704000000040000000D420000900700000008
208BA9C5EFCAA53042000074800000005A4200008F060000002461646264656638642D643662632D343838612D3961643
82D306366663062636265396331420000088000000024420000A060000000C782D617474726962757465314200000B06
0000000656616C7565314200000F80000000814200005704000000040000000D420000900700000008A3E3990370185C0
A42000074800000005A4200008F060000002461646264656638642D643662632D343838612D396164382D306366663062
636265396331420000088000000024420000A060000000C782D617474726962757465324200000B060000000656616C7
56532

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

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

- Tag: Response Header (0x42000075), Type: Structure (0x80), Data:

 - Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

 - Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 - Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

 - Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E01D2 (Wed Jan 14 16:16:34 CET 2009)
 - Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

- Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)
- Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 208BA9C5EFCAA530
- Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
- Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

 - Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

- Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute1

Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Value1
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)
 Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: A3E3990370185C0A
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute2
 Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Value2

42000076800000017842000075800000004142000065800000001A420000660100000004000000004200006701000000
 4000000624200008E080000000800000000496E01D2420000D010000004000000024200000F800000008E4200005704
 000000040000000D420000900700000008208BA9C5EFCAA5304200007A04000000040000000042000077800000005A420
 0008F060000002461646264656638642D643662632D343838612D396164382D3063666630626362653963314200000880
 000000244200000A060000000C782D617474726962757465314200000B060000000656616C7565314200000F800000008
 E4200005704000000D420000900700000008A3E3990370185C0A4200007A0400000004000000004200007780
 0000005A4200008F060000002461646264656638642D643662632D343838612D396164382D30636666306263626539633
 1420000088000000024420000A06000000C782D61747472696275746532420000B060000000656616C756532

6

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000E (Modify Attribute)
 Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: DCECF6C9D300B1EB
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute1
 Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: ModifiedValue1
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000E (Modify Attribute)
 Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 2270444ABF5E239F
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute2
 Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: ModifiedValue2

42000073800000015D42000072800000003042000065800000001A420000660100000004000000004200006701000000
 400000062420000D0100000004000000024200000F80000000894200005704000000040000000E420000900700000008

DCECF6C9D300B1EB4200007480000000624200008F060000002461646264656638642D643662632D343838612D3961643
82D30636666306263626539633142000008800000002C4200000A060000000C782D617474726962757465314200000B06
0000000E4D6F64696669656456616C7565314200000F80000000894200005704000000040000000E42000090070000000
82270444ABF5E239F4200007480000000624200008F060000002461646264656638642D643662632D343838612D396164
382D30636666306263626539633142000008800000002C4200000A060000000C782D617474726962757465324200000B0
60000000E4D6F64696669656456616C756532

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

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

Tag: Response Header (0x42000075), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E01D3 (Wed Jan 14 16:16:35 CET 2009)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000E (Modify Attribute)

Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: DCECF6C9D300B1EB

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)

Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute1

Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: ModifiedValue1

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000E (Modify Attribute)

Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 2270444ABF5E239F

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)

Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute2

Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: ModifiedValue2

42000076800000018842000075800000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E01D34200000D0100000004000000024200000F80000000964200005704
000000040000000E420000900700000008DCECF6C9D300B1EB4200007A040000000400000000420000778000000062420
0008F060000002461646264656638642D643662632D343838612D396164382D3063666630626362653963314200000880
0000002C4200000A060000000C782D617474726962757465314200000B060000000E4D6F64696669656456616C7565314
200000F80000000964200005704000000040000000E4200009007000000082270444ABF5E239F4200007A040000000400
0000004200007780000000624200008F060000002461646264656638642D643662632D343838612D396164382D3063666
6306263626539633142000008800000002C4200000A060000000C782D617474726962757465324200000B060000000E4D
6F64696669656456616C756532

7

Client B:

Delete attribute [batch]

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

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:

- Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 - Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 - Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 - Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 - Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)
- Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 - Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000F (Delete Attribute)
 - Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: A1484069949CB587
 - Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 - Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1
 - Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute1
- Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 - Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000F (Delete Attribute)
 - Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 737E3D7E11C47049
 - Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 - Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1
 - Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute2

42000073800000011D42000072800000003042000065800000001A42000066010000000400000000420000670100000004000000624200000D01000000004000000024200000F800000006942000057040000000400000000F420000900700000008A1484069949CB5874200007480000000424200008F060000002461646264656638642D643662632D343838612D396164382D3063666630626362653963314200000A060000000C782D617474726962757465314200000F800000000694200005704000000040000000F420000900700000008737E3D7E11C470494200007480000000424200008F060000002461646264656638642D643662632D343838612D396164382D3063666630626362653963314200000A060000000C782D61747472696275746532

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

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

- Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 - Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 - Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 - Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 - Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E01D3 (Wed Jan 14 16:16:35 CET 2009)
 - Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)
- Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 - Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000F (Delete Attribute)
 - Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: A1484069949CB587
 - Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 - Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 - Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1
 - Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 - Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute1
 - Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: ModifiedValue1

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000F (Delete Attribute)
 Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 737E3D7E11C47049
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute2
 Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: ModifiedValue2

```
42000076800000018842000075800000004142000065800000001A4200006601000000400000004200006701000000
4000000624200008E08000000080000000496E01D3420000D010000004000000024200000F80000000964200005704
000000040000000F420000900700000008A1484069949CB5874200007A04000000040000000420000778000000062420
0008F060000002461646264656638642D643662632D343838612D396164382D3063666630626362653963314200000880
0000002C4200000A060000000C782D617474726962757465314200000B060000000E4D6F64696669656456616C7565314
200000F80000000964200005704000000040000000F420000900700000008737E3D7E11C470494200007A040000000400
0000004200007780000000624200008F060000002461646264656638642D643662632D343838612D396164382D3063666
6306263626539633142000008800000002C4200000A060000000C782D617474726962757465324200000B060000000E4D
6F64696669656456616C756532
```

8

Client A:
Destroy (symmetric key)
In: uuidKey

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1

```
42000073800000008542000072800000003042000065800000001A4200006601000000400000004200006701000000
4000000624200000D0100000004000000014200000F8000000043420000570400000040000001442000074800000002D
4200008F060000002461646264656638642D643662632D343838612D396164382D306366663062636265396331
```

Out: uuidKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E01D3 (Wed Jan 14 16:16:35 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1

4200007680000000A342000075800000004142000065800000001A4200006601000000040000000042000067010000000
 4000000624200008E080000000800000000496E01D3420000D010000000400000001420000F80000000504200005704
 00000004000000144200007A04000000040000000042000077800000002D4200008F060000002461646264656638642D6
 43662632D343838612D396164382D306366663062636265396331

9

Client A:
Get (symmetric key)
In: uuidKey

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: adbdef8d-d6bc-488a-9ad8-0cff0bcbe9c1

42000073800000008542000072800000003042000065800000001A4200006601000000040000000042000067010000000
 400000062420000D010000000400000001420000F80000000434200005704000000040000000A42000074800000002D
 4200008F060000002461646264656638642D643662632D343838612D396164382D306366663062636265396331

Out: Operation Failed, Item Not Found

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E01D3 (Wed Jan 14 16:16:35 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000001 (Failed)
 Tag: Result Reason (0x42000079), Type: Enumeration (0x04), Data: 0x00000001 (Item Not Found)
 Tag: Result Message (0x42000078), Type: Text String (0x06), Data: No Cryptographic Object found with given Unique Identifier

4200007680000000BD42000075800000004142000065800000001A4200006601000000040000000042000067010000000
 4000000624200008E080000000800000000496E01D3420000D010000000400000001420000F800000006A4200005704
 000000040000000A4200007A0400000004000000014200007904000000040000000142000078060000003A4E6F2043727
 970746F67726170686963204F626A65637420666F756E64207769746820676976656E20556E69717565204964656E7469

	66696572
10	<p>Client A: Destroy (template) In: uuidTemplate</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data: Tag: Request Header (0x42000072), Type: Structure (0x80), Data: Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98) Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1) Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data: Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy) Tag: Request Payload (0x42000074), Type: Structure (0x80), Data: Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 7936e2b9-0185-43ab-81b1-2e644ae48996</p> <p>42000073800000008542000072800000003042000065800000001A4200006601000000040000000042000067010000000 4000000624200000D0100000004000000014200000F80000000434200005704000000040000001442000074800000002D 4200008F060000002437393336653262392D303138352D343361622D383162312D326536343461653438393936</p> <p>Out: uuidTemplate</p> <p>Tag: Response Message (0x42000076), Type: Structure (0x80), Data: Tag: Response Header (0x42000075), Type: Structure (0x80), Data: Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98) Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E01D5 (Wed Jan 14 16:16:37 CET 2009) Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1) Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data: Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy) Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success) Tag: Response Payload (0x42000077), Type: Structure (0x80), Data: Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 7936e2b9-0185-43ab-81b1-2e644ae48996</p> <p>4200007680000000A342000075800000004142000065800000001A4200006601000000040000000042000067010000000 4000000624200008E080000000800000000496E01D54200000D0100000004000000014200000F80000000504200005704 00000004000000144200007A04000000040000000042000077800000002D4200008F060000002437393336653262392D3 03138352D343361622D383162312D326536343461653438393936</p>
11	<p>Client A: Get (template) In: uuidTemplate</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data: Tag: Request Header (0x42000072), Type: Structure (0x80), Data: Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:</p>

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 7936e2b9-0185-43ab-81b1-2e644ae48996

42000073800000008542000072800000003042000065800000001A420000660100000004000000004200006701000000
 4000000624200000D0100000004000000014200000F80000000434200005704000000040000000A42000074800000002D
 4200008F060000002437393336653262392D303138352D343361622D383162312D326536343461653438393936

Out: Operation Failed, Item Not Found

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E01D6 (Wed Jan 14 16:16:38 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000001 (Failed)
 Tag: Result Reason (0x42000079), Type: Enumeration (0x04), Data: 0x00000001 (Item Not Found)
 Tag: Result Message (0x42000078), Type: Text String (0x06), Data: No Cryptographic Object found with given Unique Identifier

4200007680000000BD42000075800000004142000065800000001A420000660100000004000000004200006701000000
 4000000624200008E080000000800000000496E01D64200000D0100000004000000014200000F800000006A4200005704
 000000040000000A4200007A0400000004000000014200007904000000040000000142000078060000003A4E6F2043727
 970746F67726170686963204F626A65637420666F756E64207769746820676976656E20556E69717565204964656E7469
 66696572

3.2 Use-case: Asynchronous Locate

This use-case tests the asynchronous capabilities of KMIP using locate.

Time	Client A
1	Client A: Create (symmetric key) In: objectType = '00000002', attributes={ Name={ Name='Key1', NameType='00000001' }, ObjectGroup='Group1', CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='00000004' }

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:

- Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 - Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 - Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 - Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 - Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
- Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 - Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000001 (Create)
 - Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 - Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
 - Tag: Template-Attribute (0x4200008D), Type: Structure (0x80), Data:
 - Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 - Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name
 - Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:
 - Tag: Name Value (0x42000050), Type: Text String (0x06), Data: Key1
 - Tag: Name Type (0x4200004F), Type: Enumeration (0x04), Data: 0x00000001 (Uninterpreted text string)
 - Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 - Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Group
 - Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Group1
 - Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 - Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Algorithm
 - Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000003 (AES)
 - Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 - Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Length
 - Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x00000080 (128)
 - Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 - Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Usage Mask
 - Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x00000004 (Encrypt)

```
42000073800000017442000072800000003042000065800000001A4200006601000000040000000042000067010000000
4000000624200000D0100000004000000014200000F80000001324200005704000000040000000142000074800000011C
420000520400000004000000024200008D8000000106420000088000000030420000A06000000044E616D654200000B8
00000001A4200005006000000044B6579314200004F040000000400000001420000880000000244200000A060000000C
4F626A6563742047726F75704200000B060000000647726F75703142000008800000002D420000A06000000174372797
0746F6772617068696320416C676F726974686D4200000B0400000004000000034200008800000002A420000A060000
001443727970746F67726170686963204C656E6774684200000B0100000004000000804200008800000002E420000A0
60000001843727970746F67726170686963205573616765204D61736B4200000B010000000400000004
```

Out: objectType = '00000002', uuidKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

- Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 - Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 - Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 - Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 - Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0406 (Wed Jan 14 16:25:58 CET 2009)
 - Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000001 (Create)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: a8397a68-722b-4908-8f79-alb9be0fccaf

4200007680000000B042000075800000004142000065800000001A4200006601000000040000000042000067010000000
 4000000624200008E080000000800000000496E0406420000D010000000400000001420000F800000005D4200005704
 00000004000000014200007A04000000040000000042000077800000003A420000520400000004000000024200008F060
 000002461383339376136382D373232622D343930382D386637392D613162396265306663636166

2

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Asynchronous Indicator (0x42000007), Type: Boolean (0x05), Data: TRUE
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Type
 Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name
 Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:
 Tag: Name Value (0x42000050), Type: Text String (0x06), Data: Key1
 Tag: Name Type (0x4200004F), Type: Enumeration (0x04), Data: 0x00000001 (Uninterpreted text string)

4200007380000000C542000072800000003A42000065800000001A4200006601000000040000000042000067010000000
 4000000624200007050000000101420000D010000000400000001420000F8000000079420000570400000004000000
 08420000748000000063420000088000000021420000A060000000B4F626A6563742054797065420000B04000000040
 0000002420000088000000030420000A06000000044E616D65420000B800000001A42000050060000000044B65793142
 00004F040000000400000001

Out: asyncCorrValue1

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0407 (Wed Jan 14 16:25:59 CET 2009)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000002 (Pending)

Tag: Asynchronous Correlation Value (0x42000006), Type: Octet String (0x07), Data: 6B41EF71666A081E

420000768000000007E42000075800000004142000065800000001A420000660100000004000000004200006701000000004000000624200008E080000000800000000496E04074200000D0100000004000000014200000F800000002B420000570400000004000000084200007A0400000004000000024200000607000000086B41EF71666A081E

3

Client B:

Poll*

In: asyncCorrValue1

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:

Tag: Request Header (0x42000072), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000001A (Poll)

Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:

Tag: Asynchronous Correlation Value (0x42000006), Type: Octet String (0x07), Data: 6B41EF71666A081E

420000738000000006942000072800000003042000065800000001A420000660100000004000000004200006701000000004000000624200000D0100000004000000014200000F80000000274200005704000000040000001A4200007480000000011420000607000000086B41EF71666A081E

Out: uuidKey1

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

Tag: Response Header (0x42000075), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0407 (Wed Jan 14 16:25:59 CET 2009)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)

Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: a8397a68-722b-4908-8f79-alb9be0fccaf

42000076800000000A342000075800000004142000065800000001A420000660100000004000000004200006701000000004000000624200008E080000000800000000496E04074200000D0100000004000000014200000F80000000504200005704

00000004000000084200007A04000000040000000042000077800000002D4200008F060000002461383339376136382D373232622D343930382D386637392D613162396265306663636166

4

Client B:
Get (symmetric key)
In: uuidKey1

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: a8397a68-722b-4908-8f79-alb9be0fccaf

42000073800000008542000072800000003042000065800000001A4200006601000000040000000042000067010000000400000062420000D0100000004000000014200000F80000000434200005704000000040000000A42000074800000002D4200008F060000002461383339376136382D373232622D343930382D386637392D613162396265306663636166

Out: objectType = '00000002', uuidKey1, symmetricKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0407 (Wed Jan 14 16:25:59 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: a8397a68-722b-4908-8f79-alb9be0fccaf
 Tag: Symmetric Key (0x4200008A), Type: Structure (0x80), Data:
 Tag: Key Block (0x4200003C), Type: Structure (0x80), Data:
 Tag: Key Value Type (0x42000040), Type: Enumeration (0x04), Data: 0x00000001
 Tag: Key Value (0x4200003F), Type: Structure (0x80), Data:
 Tag: Key Material (0x4200003D), Type: Octet String (0x07), Data: 0D3AA84EAD3FD5B82E776697CEFD3102
 Tag: Cryptographic Algorithm (0x42000025), Type: Enumeration (0x04), Data: 0x00000003 (AES)
 Tag: Cryptographic Length (0x42000026), Type: Integer (0x01), Data: 0x00000080 (128)

42000076800000010B42000075800000004142000065800000001A42000066010000000400000000420000670100000004000000624200008E080000000800000000496E0407420000D0100000004000000014200000F80000000B84200005704

000000040000000A4200007A040000000400000000420000778000000095420000520400000004000000024200008F060
000002461383339376136382D373232622D343930382D386637392D6131623962653066636361664200008A8000000052
4200003C8000000049420000400400000004000000014200003F80000000194200003D07000000100D3AA84EAD3FD5B82
E776697CEFD31024200002504000000040000000342000026010000000400000080

5	<p>Client B:</p> <p>Locate (symmetric key by group)</p> <p>In: asynchronousIndicator='TRUE', attributes={ objectType = '0000002', ObjectGroup='Group1' }</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data:</p> <p> Tag: Request Header (0x42000072), Type: Structure (0x80), Data:</p> <p> Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:</p> <p> Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)</p> <p> Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)</p> <p> Tag: Asynchronous Indicator (0x42000007), Type: Boolean (0x05), Data: TRUE</p> <p> Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)</p> <p> Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:</p> <p> Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)</p> <p> Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:</p> <p> Tag: Attribute (0x42000008), Type: Structure (0x80), Data:</p> <p> Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Type</p> <p> Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)</p> <p> Tag: Attribute (0x42000008), Type: Structure (0x80), Data:</p> <p> Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Group</p> <p> Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Group1</p> <p>4200007380000000B942000072800000003A42000065800000001A420000660100000004000000042000067010000000 40000006242000007050000000101420000D010000000400000014200000F800000006D420000570400000004000000 0842000074800000005742000088000000021420000A060000000B4F626A65637420547970654200000B04000000040 000000242000088000000024420000A060000000C4F626A6563742047726F75704200000B060000000647726F757031</p> <p>Out: asyncCorrValue2</p> <p>Tag: Response Message (0x42000076), Type: Structure (0x80), Data:</p> <p> Tag: Response Header (0x42000075), Type: Structure (0x80), Data:</p> <p> Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:</p> <p> Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)</p> <p> Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)</p> <p> Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0407 (Wed Jan 14 16:25:59 CET 2009)</p> <p> Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)</p> <p> Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:</p> <p> Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)</p> <p> Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000002 (Pending)</p> <p> Tag: Asynchronous Correlation Value (0x42000006), Type: Octet String (0x07), Data: ECA9B3F4F4D5E15F</p> <p>420000768000000007E42000075800000004142000065800000001A420000660100000004000000042000067010000000 4000000624200008E080000000800000000496E0407420000D010000000400000014200000F800000002B4200005704 00000004000000084200007A040000000400000002420000060700000008ECA9B3F4F4D5E15F</p>
---	--

6	<p>Client B: Poll* In: asyncCorrValue2</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data: Tag: Request Header (0x42000072), Type: Structure (0x80), Data: Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98) Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1) Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data: Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000001A (Poll) Tag: Request Payload (0x42000074), Type: Structure (0x80), Data: Tag: Asynchronous Correlation Value (0x42000006), Type: Octet String (0x07), Data: ECA9B3F4F4D5E15F</p> <p>42000073800000006942000072800000003042000065800000001A4200006601000000040000000042000067010000000 4000000624200000D0100000004000000014200000F80000000274200005704000000040000001A420000748000000011 420000060700000008ECA9B3F4F4D5E15F</p> <p>Out: uuidKey2</p> <p>Tag: Response Message (0x42000076), Type: Structure (0x80), Data: Tag: Response Header (0x42000075), Type: Structure (0x80), Data: Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98) Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0408 (Wed Jan 14 16:26:00 CET 2009) Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1) Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data: Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate) Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success) Tag: Response Payload (0x42000077), Type: Structure (0x80), Data: Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: a8397a68-722b-4908- 8f79-alb9be0fccaf</p> <p>42000076800000000A342000075800000004142000065800000001A4200006601000000040000000042000067010000000 4000000624200008E080000000800000000496E0408420000D0100000004000000014200000F80000000504200005704 00000004000000084200007A04000000040000000042000077800000002D4200008F060000002461383339376136382D3 73232622D343930382D386637392D613162396265306663636166</p>
7	<p>Client B: Get (symmetric key) In: uuidKey2</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data: Tag: Request Header (0x42000072), Type: Structure (0x80), Data: Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)</p>

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: a8397a68-722b-4908-8f79-alb9be0fccaf

42000073800000008542000072800000003042000065800000001A4200006601000000040000000042000067010000000
 4000000624200000D0100000004000000014200000F80000000434200005704000000040000000A420000748000000002D
 4200008F060000002461383339376136382D373232622D343930382D386637392D613162396265306663636166

Out: objectType = '00000002', uuidKey2, symmetricKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0408 (Wed Jan 14 16:26:00 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: a8397a68-722b-4908-8f79-alb9be0fccaf
 Tag: Symmetric Key (0x4200008A), Type: Structure (0x80), Data:
 Tag: Key Block (0x4200003C), Type: Structure (0x80), Data:
 Tag: Key Value Type (0x42000040), Type: Enumeration (0x04), Data: 0x00000001
 Tag: Key Value (0x4200003F), Type: Structure (0x80), Data:
 Tag: Key Material (0x4200003D), Type: Octet String (0x07), Data: 0D3AA84EAD3FD5B82E776697CEFD3102
 Tag: Cryptographic Algorithm (0x42000025), Type: Enumeration (0x04), Data: 0x00000003 (AES)
 Tag: Cryptographic Length (0x42000026), Type: Integer (0x01), Data: 0x00000080 (128)

42000076800000010B42000075800000004142000065800000001A4200006601000000040000000042000067010000000
 4000000624200008E080000000800000000496E04084200000D0100000004000000014200000F80000000B84200005704
 000000040000000A4200007A040000000400000000420000778000000095420000520400000004000000024200008F060
 000002461383339376136382D373232622D343930382D386637392D6131623962653066636361664200008A8000000052
 4200003C8000000049420000400400000004000000014200003F80000000194200003D07000000100D3AA84EAD3FD5B82
 E776697CEFD31024200002504000000040000000342000026010000000400000080

8	<p>Client B: Locate (symmetric key by name) In: asynchronousIndicator='TRUE', attributes={ objectType = '00000002', Name= { Name='Key1', NameType='00000001' } }</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data:</p>
---	---

Tag: Request Header (0x42000072), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Asynchronous Indicator (0x42000007), Type: Boolean (0x05), Data: TRUE

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)

Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Type

Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name

Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:

Tag: Name Value (0x42000050), Type: Text String (0x06), Data: Key1

Tag: Name Type (0x4200004F), Type: Enumeration (0x04), Data: 0x00000001 (Uninterpreted text string)

4200007380000000C542000072800000003A42000065800000001A4200006601000000040000000042000067010000000
400000062420000070500000001014200000D0100000004000000014200000F8000000079420000570400000004000000
08420000748000000063420000880000000214200000A060000000B4F626A65637420547970654200000B04000000040
00000024200000880000000304200000A06000000044E616D654200000B800000001A42000050060000000044B65793142
00004F040000000400000001

Out: asyncCorrValue5

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

Tag: Response Header (0x42000075), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0408 (Wed Jan 14 16:26:00 CET 2009)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000002 (Pending)

Tag: Asynchronous Correlation Value (0x42000006), Type: Octet String (0x07), Data: 33E3FAF14A6358E7

42000076800000007E42000075800000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E08000000080000000496E04084200000D0100000004000000014200000F800000002B4200005704
00000004000000084200007A04000000040000000242000006070000000833E3FAF14A6358E7

9	<p>Client B:</p> <p>Cancel</p> <p>In: asyncCorrValue5</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data:</p> <p>Tag: Request Header (0x42000072), Type: Structure (0x80), Data:</p>
---	---

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000019 (Cancel)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Asynchronous Correlation Value (0x42000006), Type: Octet String (0x07), Data:
 33E3FAF14A6358E7

42000073800000006942000072800000003042000065800000001A420000660100000004000000004200006701000000
 4000000624200000D0100000004000000014200000F800000002742000057040000000400000019420000748000000011
 42000006070000000833E3FAF14A6358E7

Out: asyncCorrValue5, CancelResult='00000001'

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0408 (Wed Jan 14
 16:26:00 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000019 (Cancel)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Asynchronous Correlation Value (0x42000006), Type: Octet String (0x07), Data:
 33E3FAF14A6358E7
 Tag: Cancellation Result (0x42000012), Type: Enumeration (0x04), Data: 0x00000001
 (Cancelled)

420000768000000009442000075800000004142000065800000001A420000660100000004000000004200006701000000
 4000000624200008E080000000800000000496E04084200000D0100000004000000014200000F80000000414200005704
 00000004000000194200007A0400000004000000042000077800000001E42000006070000000833E3FAF14A6358E7420
 00012040000000400000001

10

Client A:
 Destroy (symmetric key)
 In: uuidKey

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: a8397a68-722b-4908-

	<p>8f79-alb9be0fccaf</p> <p>42000073800000008542000072800000003042000065800000001A4200006601000000040000000042000067010000000 4000000624200000D0100000004000000014200000F80000000434200005704000000040000001442000074800000002D 4200008F060000002461383339376136382D373232622D343930382D386637392D613162396265306663636166</p> <p>Out: uuidKey</p> <p>Tag: Response Message (0x42000076), Type: Structure (0x80), Data: Tag: Response Header (0x42000075), Type: Structure (0x80), Data: Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98) Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0408 (Wed Jan 14 16:26:00 CET 2009) Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1) Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data: Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy) Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success) Tag: Response Payload (0x42000077), Type: Structure (0x80), Data: Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: a8397a68-722b-4908-8f79-alb9be0fccaf</p> <p>4200007680000000A342000075800000004142000065800000001A4200006601000000040000000042000067010000000 4000000624200008E080000000800000000496E04084200000D0100000004000000014200000F80000000504200005704 00000004000000144200007A04000000040000000042000077800000002D4200008F060000002461383339376136382D3 73232622D343930382D386637392D613162396265306663636166</p>
--	--

* = executed until response is ready

4 Key life cycle support

4.1 Use-case: Revoke scenario

This use-case tests the revocation aspect of the key life cycle support in KMIP.

Time	Client A
0	<p>Client A: Create (symmetric key) In: objectType = '00000002', attributes={ Name={ Name='Key1', NameType='00000001' }, CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='00000004' }</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data: Tag: Request Header (0x42000072), Type: Structure (0x80), Data:</p>

```

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
  Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
  Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
  Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000001 (Create)
  Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
    Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
    Tag: Template-Attribute (0x4200008D), Type: Structure (0x80), Data:
      Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
        Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name
        Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:
          Tag: Name Value (0x42000050), Type: Text String (0x06), Data: Key1
          Tag: Name Type (0x4200004F), Type: Enumeration (0x04), Data: 0x00000001
(Uninterpreted text string)
        Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
          Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic
Algorithm
          Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000003 (AES)
        Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
          Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Length
          Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x00000080 (128)
        Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
          Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x00000004 (Encrypt)

4200007380000001474200007280000000304200006580000001A4200006601000000040000000042000067010000000
4000000624200000D0100000004000000014200000F8000000105420000570400000004000000014200007480000000EF
420000520400000004000000024200008D80000000D94200000880000000304200000A06000000044E616D654200000B8
00000001A42000050060000000044B6579314200004F04000000040000000142000008800000002D4200000A0600000017
43727970746F6772617068696320416C676F726974686D4200000B04000000040000000342000008800000002A4200000
A060000001443727970746F67726170686963204C656E6774684200000B010000000400000008042000008800000002E42
00000A060000001843727970746F67726170686963205573616765204D61736B4200000B010000000400000004

```

Out: objectType = '00000002', uuidKey

```

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
  Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
    Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
      Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
    Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B5C (Wed Jan 14
16:57:16 CET 2009)
    Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
  Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
    Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000001 (Create)
    Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
      Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-
b5a6-7728bba4166f

```

4200007680000000B042000075800000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E0B5C420000D010000000400000001420000F800000005D4200005704
00000004000000014200007A04000000040000000042000077800000003A420000520400000004000000024200008F060
000002436613637663664392D373363632D343838322D623561362D373732386262613431363666

1

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000B (Get Attributes)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: State

420000738000000009342000072800000003042000065800000001A4200006601000000040000000042000067010000000
400000062420000D010000000400000001420000F80000000514200005704000000040000000B42000074800000003B
4200008F060000002436613637663664392D373363632D343838322D623561362D3737323862626134313636664200000
A06000000055374617465

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B5D (Wed Jan 14 16:57:17 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000B (Get Attributes)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: State
 Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000001 (Pre-Active)

42000076800000000C742000075800000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E0B5D420000D010000000400000001420000F80000000744200005704
000000040000000B4200007A0400000004000000004200007780000000514200008F060000002436613637663664392D3
73363632D343838322D623561362D37373238626261343136366642000008800000001B4200000A060000000553746174

65420000B040000000400000001

2

Client A:

Add attribute

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:

Tag: Request Header (0x42000072), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)

Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Activation Date

Tag: Attribute Value (0x4200000B), Type: Date-Time (0x08), Data: 0x0000000000000002 (Thu Jan 01 01:00:02 CET 1970)

4200007380000000B742000072800000003042000065800000001A4200006601000000040000000042000067010000000
4000000624200000D0100000004000000014200000F80000000754200005704000000040000000D420000748000000005F
4200008F060000002436613637663664392D373363632D343838322D623561362D3737323862626134313636664200000
880000000294200000A060000000F41637469766174696F6E20446174654200000B08000000080000000000000000

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

Tag: Response Header (0x42000075), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B5D (Wed Jan 14 16:57:17 CET 2009)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)

Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Activation Date

Tag: Attribute Value (0x4200000B), Type: Date-Time (0x08), Data: 0x0000000000000002 (Thu Jan 01 01:00:02 CET 1970)

42000076800000000D5420000758000000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E0B5D4200000D0100000004000000014200000F80000000824200005704
000000040000000D4200007A04000000040000000042000077800000005F4200008F060000002436613637663664392D3
73363632D343838322D623561362D3737323862626134313636664200000880000000294200000A060000000F41637469

766174696F6E2044617465420000B0800000080000000000000002

3

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000B (Get Attributes)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: State

4200007380000009342000072800000003042000065800000001A4200006601000000040000000042000067010000000
4000000624200000D0100000004000000014200000F80000000514200005704000000040000000B42000074800000003B
4200008F060000002436613637663664392D373363632D343838322D623561362D3737323862626134313636664200000
A06000000055374617465

Out: uuidKey, attribute={ State='00000002' }

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B5D (Wed Jan 14 16:57:17 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000B (Get Attributes)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: State
 Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000002 (Active)

4200007680000000C742000075800000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E0B5D4200000D0100000004000000014200000F80000000744200005704
000000040000000B4200007A0400000004000000004200007780000000514200008F060000002436613637663664392D3
73363632D343838322D623561362D37373238626261343136366642000008800000001B4200000A060000000553746174
654200000B040000000400000002

4

Client B:
Locate (symmetric key by name)

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)
Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Type
Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name
Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:
Tag: Name Value (0x42000050), Type: Text String (0x06), Data: Key1
Tag: Name Type (0x4200004F), Type: Enumeration (0x04), Data: 0x00000001 (Uninterpreted text string)

4200007380000000BB42000072800000003042000065800000001A4200006601000000040000000042000067010000000
4000000624200000D0100000004000000014200000F800000007942000057040000000400000008420000748000000063
42000008800000000214200000A060000000B4F626A65637420547970654200000B0400000004000000024200000880000
000304200000A06000000044E616D654200000B800000001A4200005006000000044B6579314200004F04000000040000
0001

Out: uuidKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B5E (Wed Jan 14 16:57:18 CET 2009)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)
Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f

42000076800000000A342000075800000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E0B5E4200000D0100000004000000014200000F80000000504200005704
00000004000000084200007A04000000040000000042000077800000002D4200008F0600000002436613637663664392D3
73363632D343838322D623561362D373732386262613431363666

5

Client B:
Get (symmetric key)

In: uuidKey

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f

42000073800000008542000072800000003042000065800000001A4200006601000000040000000042000067010000000
4000000624200000D0100000004000000014200000F80000000434200005704000000040000000A42000074800000002D
4200008F060000002436613637663664392D373363632D343838322D623561362D373732386262613431363666

Out: objectType = '00000002', uuidKey, symmetricKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B5E (Wed Jan 14 16:57:18 CET 2009)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
Tag: Symmetric Key (0x4200008A), Type: Structure (0x80), Data:
Tag: Key Block (0x4200003C), Type: Structure (0x80), Data:
Tag: Key Value Type (0x42000040), Type: Enumeration (0x04), Data: 0x00000001
Tag: Key Value (0x4200003F), Type: Structure (0x80), Data:
Tag: Key Material (0x4200003D), Type: Octet String (0x07), Data: 59E8D268CB2FD53E50C79BE91137406E
Tag: Cryptographic Algorithm (0x42000025), Type: Enumeration (0x04), Data: 0x00000003 (AES)
Tag: Cryptographic Length (0x42000026), Type: Integer (0x01), Data: 0x00000080 (128)

420000768000000010B42000075800000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E08000000080000000496E0B5E4200000D0100000004000000014200000F80000000B84200005704
000000040000000A4200007A040000000400000000420000778000000095420000520400000004000000024200008F060
000002436613637663664392D373363632D343838322D623561362D3737323862626134313636664200008A8000000052
4200003C8000000049420000400400000004000000014200003F80000000194200003D070000001059E8D268CB2FD53E5
0C79BE91137406E4200002504000000040000000342000026010000000400000080

6	<p>Client B: Revoke (symmetric key as compromised) In: uuidKey, RevocationReason='0000002', CompromiseOccurrenceTime='6'</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data: Tag: Request Header (0x42000072), Type: Structure (0x80), Data: Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98) Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1) Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data: Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000013 (Revoke) Tag: Request Payload (0x42000074), Type: Structure (0x80), Data: Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f Tag: Revocation Reason (0x4200007C), Type: Structure (0x80), Data: Tag: Revocation Reason Code (0x4200007D), Type: Enumeration (0x04), Data: 0x00000001 (Key Compromise) Tag: Compromise Occurrence Date (0x4200001E), Type: Date-Time (0x08), Data: 0x0000000000000006 (Thu Jan 01 01:00:06 CET 1970)</p> <p>4200007380000000AC42000072800000003042000065800000001A4200006601000000040000000042000067010000000400000062420000D0100000004000000014200000F800000006A420000570400000004000000134200007480000000544200008F060000002436613637663664392D373363632D343838322D623561362D3737323862626134313636664200007C800000000D4200007D0400000004000000014200001E08000000080000000000000000000000</p> <p>Out: uuidKey</p> <p>Tag: Response Message (0x42000076), Type: Structure (0x80), Data: Tag: Response Header (0x42000075), Type: Structure (0x80), Data: Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98) Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B5E (Wed Jan 14 16:57:18 CET 2009) Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1) Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data: Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000013 (Revoke) Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success) Tag: Response Payload (0x42000077), Type: Structure (0x80), Data: Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f</p> <p>4200007680000000A342000075800000004142000065800000001A42000066010000000400000000420000670100000004000000624200008E080000000800000000496E0B5E420000D0100000004000000014200000F8000000050420000570400000004000000134200007A04000000040000000042000077800000002D4200008F0600000002436613637663664392D373363632D343838322D623561362D373732386262613431363666</p>
7	<p>Client B: Get attribute In: uuidKey, attributeName={ 'State' }</p>

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000B (Get Attributes)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: State

42000073800000009342000072800000003042000065800000001A4200006601000000040000000042000067010000000
 4000000624200000D0100000004000000014200000F80000000514200005704000000040000000B42000074800000003B
 4200008F060000002436613637663664392D373363632D343838322D623561362D373732386262613431363666420000
 A06000000055374617465

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B5F (Wed Jan 14 16:57:19 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000B (Get Attributes)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: State
 Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000004 (Compromised)

42000076800000000C742000075800000004142000065800000001A4200006601000000040000000042000067010000000
 4000000624200008E080000000800000000496E0B5F4200000D0100000004000000014200000F80000000744200005704
 000000040000000B4200007A0400000004000000004200007780000000514200008F060000002436613637663664392D3
 73363632D343838322D623561362D37373238626261343136366642000008800000001B4200000A0600000000553746174
 654200000B040000000400000004

8 Client A:
 Get attribute list
 In: uuidKey

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000C (Get Attribute List)
Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f

42000073800000008542000072800000003042000065800000001A420000660100000004000000004200006701000000
4000000624200000D0100000004000000014200000F80000000434200005704000000040000000C42000074800000002D
4200008F060000002436613637663664392D373363632D343838322D623561362D373732386262613431363666

Out: uuidKey, attributes = { * }

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B5F (Wed Jan 14 16:57:19 CET 2009)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000C (Get Attribute List)
Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Length
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Algorithm
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: State
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Compromise Occurrence
Date
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Compromise Date
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Initial Date
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Activation Date
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Revocation Reason
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Unique Identifier
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Usage Mask
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Type
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Last Changed Date

4200007680000001E642000075800000004142000065800000001A420000660100000004000000004200006701000000
4000000624200008E080000000800000000496E0B5F4200000D0100000004000000014200000F80000001934200005704
000000040000000C4200007A0400000004000000004200007780000001704200008F060000002436613637663664392D3
7363632D343838322D623561362D3737323862626134313636664200000A060000001443727970746F67726170686963
204C656E6774684200000A060000001743727970746F6772617068696320416C676F726974686D4200000A06000000055
3746174654200000A060000001A436F6D70726F6D697365204F6363757272656E636520446174654200000A060000000F
436F6D70726F6D69736520446174654200000A060000000C496E697469616C20446174654200000A06000000F4163746
9766174696F6E20446174654200000A06000000115265766F636174696F6E20526561736F6E4200000A0600000011556E

69717565204964656E7469666965724200000A06000000044E616D654200000A060000001843727970746F67726170686
963205573616765204D61736B4200000A060000000B4F626A65637420547970654200000A06000000114C617374204368
616E6765642044617465

9

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000B (Get Attributes)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-
b5a6-7728bba4166f
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: State

42000073800000009342000072800000003042000065800000001A4200006601000000040000000042000067010000000
4000000624200000D0100000004000000014200000F800000000514200005704000000040000000B420000748000000003B
4200008F060000002436613637663664392D373363632D343838322D623561362D3737323862626134313636664200000
A060000000055374617465

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B5F (Wed Jan 14
16:57:19 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000B (Get Attributes)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-
b5a6-7728bba4166f
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: State
 Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000004
(Compromised)

42000076800000000C742000075800000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E0B5F420000D0100000004000000014200000F80000000744200005704
000000040000000B4200007A0400000004000000004200007780000000514200008F060000002436613637663664392D3
73363632D343838322D623561362D37373238626261343136366642000008800000001B4200000A060000000553746174
654200000B040000000400000004

Client A:

Add attribute [batch]

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

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:

Tag: Request Header (0x42000072), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)

Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 989D9CCCF325C9CB

Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute1

Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Value1

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)

Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: F291145F8553CD75

Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute2

Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Value2

```
42000073800000014D4200007280000000304200006580000001A4200006601000000400000004200006701000000
40000062420000D0100000040000002420000F80000008142000057040000004000000D420000900700000008
989D9CCCF325C9CB42000074800000005A4200008F060000002436613637663664392D373363632D343838322D6235613
62D37373238626261343136366642000088000000024420000A060000000C782D61747472696275746531420000B06
000000656616C756531420000F800000008142000057040000004000000D420000900700000008F291145F8553CD7
54200007480000005A4200008F060000002436613637663664392D373363632D343838322D623561362D373732386262
61343136366642000088000000024420000A060000000C782D61747472696275746532420000B060000000656616C7
56532
```

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

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

Tag: Response Header (0x42000075), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B5F (Wed Jan 14 16:57:19 CET 2009)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)

Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 989D9CCCCF325C9CB

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)

Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute1

Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Value1

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)

Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: F291145F8553CD75

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)

Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute2

Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: Value2

42000076800000017842000075800000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E0B5F420000D0100000004000000024200000F800000008E4200005704
000000040000000D420000900700000008989D9CCCCF325C9CB4200007A04000000040000000042000077800000005A420
008F060000002436613637663664392D373363632D343838322D623561362D373732386262613431363666420000880
000000244200000A060000000C782D617474726962757465314200000B060000000656616C7565314200000F800000008
E420000570400000004000000D420000900700000008F291145F8553CD754200007A0400000004000000004200007780
0000005A4200008F060000002436613637663664392D373363632D343838322D623561362D37373238626261343136366
6420000880000000244200000A060000000C782D617474726962757465324200000B060000000656616C756532

11

Client A:

Modify attribute [batch]

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

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:

Tag: Request Header (0x42000072), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000E (Modify Attribute)

Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 3AF6DF291C0B4C39

Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute1

Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: ModifiedValue1

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000E (Modify Attribute)

Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: EC9FFF5CFA921715
Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute2
Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: ModifiedValue2

42000073800000015D42000072800000003042000065800000001A4200006601000000040000000042000067010000000
4000000624200000D0100000004000000024200000F80000000894200005704000000040000000E420000900700000008
3AF6DF291C0B4C394200007480000000624200008F060000002436613637663664392D373363632D343838322D6235613
62D3737323862626134313636664200008800000002C4200000A060000000C782D61747472696275746531420000B06
0000000E4D6F64696669656456616C7565314200000F80000000894200005704000000040000000E42000090070000000
8EC9FFF5CFA9217154200007480000000624200008F060000002436613637663664392D373363632D343838322D623561
362D3737323862626134313636664200008800000002C4200000A060000000C782D61747472696275746532420000B0
60000000E4D6F64696669656456616C756532

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

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B60 (Wed Jan 14 16:57:20 CET 2009)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000E (Modify Attribute)
Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 3AF6DF291C0B4C39
Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute1
Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: ModifiedValue1
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000E (Modify Attribute)
Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: EC9FFF5CFA921715
Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute2
Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: ModifiedValue2

420000768000000188420000758000000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E0B604200000D0100000004000000024200000F80000000964200005704
000000040000000E4200009007000000083AF6DF291C0B4C394200007A04000000040000000420000778000000062420
008F060000002436613637663664392D373363632D343838322D623561362D373732386262613431363666420000880

0000002C4200000A060000000C782D617474726962757465314200000B060000000E4D6F64696669656456616C7565314
200000F80000000964200005704000000040000000E420000900700000008EC9FFF5CFA9217154200007A040000000400
0000004200007780000000624200008F060000002436613637663664392D373363632D343838322D623561362D3737323
8626261343136366642000008800000002C4200000A060000000C782D617474726962757465324200000B060000000E4D
6F64696669656456616C756532

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000F (Delete Attribute)
Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: BAA7130E892835BB
Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute1
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000F (Delete Attribute)
Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 7D4CBEEC3CAAD205
Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute2

42000073800000011D42000072800000003042000065800000001A4200006601000000040000000042000067010000000
4000000624200000D0100000004000000024200000F80000000694200005704000000040000000F420000900700000008
BAA7130E892835BB4200007480000000424200008F060000002436613637663664392D373363632D343838322D6235613
62D3737323862626134313636664200000A060000000C782D617474726962757465314200000F80000000694200005704
000000040000000F4200009007000000087D4CBEEC3CAAD2054200007480000000424200008F060000002436613637663
664392D373363632D343838322D623561362D3737323862626134313636664200000A060000000C782D61747472696275
746532

Out: uuidKey, attributeNames={ 'x-attribute1' }
Out: uuidKey, attributeNames={ 'x-attribute2' }

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B61 (Wed Jan 14
16:57:21 CET 2009)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000F (Delete Attribute)
 Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: BAA7130E892835BB
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute1
 Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: ModifiedValue1
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000F (Delete Attribute)
 Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 7D4CBEEC3CAAD205
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-attribute2
 Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: ModifiedValue2

```
42000076800000018842000075800000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E0B61420000D0100000004000000024200000F80000000964200005704
000000040000000F420000900700000008BAA7130E892835BB4200007A040000000400000000420000778000000062420
0008F060000002436613637663664392D373363632D343838322D623561362D373732386262613431363666420000880
0000002C420000A060000000C782D61747472696275746531420000B060000000E4D6F64696669656456616C7565314
200000F8000000964200005704000000040000000F4200009007000000087D4CBEEC3CAAD2054200007A040000000400
000004200007780000000624200008F060000002436613637663664392D373363632D343838322D623561362D3737323
862626134313636664200008800000002C420000A060000000C782D61747472696275746532420000B060000000E4D
6F64696669656456616C756532
```

13

Client A:
 Get (symmetric key)
 In: uuidKey

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f

```
42000073800000008542000072800000003042000065800000001A4200006601000000040000000042000067010000000
400000062420000D0100000004000000014200000F80000000434200005704000000040000000A42000074800000002D
4200008F060000002436613637663664392D373363632D343838322D623561362D373732386262613431363666
```

Out: objectType = '00000002', uuidKey, symmetricKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

Tag: Response Header (0x42000075), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B61 (Wed Jan 14 16:57:21 CET 2009)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)

Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f

Tag: Symmetric Key (0x4200008A), Type: Structure (0x80), Data:

Tag: Key Block (0x4200003C), Type: Structure (0x80), Data:

Tag: Key Value Type (0x42000040), Type: Enumeration (0x04), Data: 0x00000001

Tag: Key Value (0x4200003F), Type: Structure (0x80), Data:

Tag: Key Material (0x4200003D), Type: Octet String (0x07), Data: 59E8D268CB2FD53E50C79BE91137406E

Tag: Cryptographic Algorithm (0x42000025), Type: Enumeration (0x04), Data: 0x00000003 (AES)

Tag: Cryptographic Length (0x42000026), Type: Integer (0x01), Data: 0x00000080 (128)

42000076800000010B42000075800000004142000065800000001A4200006601000000040000000420000670100000004000000624200008E080000000800000000496E0B61420000D01000000400000001420000F80000000B8420000570400000040000000A4200007A040000000400000000420000778000000095420000520400000004000000024200008F060000002436613637663664392D373363632D343838322D623561362D3737323862626134313636664200008A80000000524200003C8000000049420000400400000004000000014200003F80000000194200003D070000001059E8D268CB2FD53E50C79BE91137406E4200002504000000040000000342000026010000000400000080

14

Client A:
Destroy (symmetric key)
In: uuidKey

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:

Tag: Request Header (0x42000072), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy)

Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f

42000073800000008542000072800000003042000065800000001A420000660100000004000000042000067010000000400000062420000D010000000400000001420000F800000004342000057040000000400000014420000748000000002D4200008F0600000002436613637663664392D373363632D343838322D623561362D373732386262613431363666

	<p>Out: uuidKey</p> <p>Tag: Response Message (0x42000076), Type: Structure (0x80), Data:</p> <p style="padding-left: 20px;">Tag: Response Header (0x42000075), Type: Structure (0x80), Data:</p> <p style="padding-left: 40px;">Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:</p> <p style="padding-left: 60px;">Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)</p> <p style="padding-left: 60px;">Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)</p> <p style="padding-left: 40px;">Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0B61 (Wed Jan 14 16:57:21 CET 2009)</p> <p style="padding-left: 40px;">Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)</p> <p style="padding-left: 20px;">Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:</p> <p style="padding-left: 40px;">Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy)</p> <p style="padding-left: 40px;">Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)</p> <p style="padding-left: 40px;">Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:</p> <p style="padding-left: 60px;">Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 6a67f6d9-73cc-4882-b5a6-7728bba4166f</p> <p>42000076800000000A3420000758000000004142000065800000001A42000066010000000400000000420000670100000004000000624200008E080000000800000000496E0B614200000D010000004000000014200000F800000005042000057040000004000000144200007A04000000040000000042000077800000002D4200008F060000002436613637663664392D373363632D343838322D623561362D373732386262613431363666</p>
--	--

5 Auditing and reporting

5.1 Use-case: Get usage allocation scenario

This use-case tests the usage management functionality of KMIP.

Time	Client A
0	<p>Client A:</p> <p>Create (symmetric key)</p> <p>In: objectType = '00000002', attributes={ Name={ Name='Key1', NameType='00000001' }, ObjectGroup='Group1', CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='00000004' }</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data:</p> <p style="padding-left: 20px;">Tag: Request Header (0x42000072), Type: Structure (0x80), Data:</p> <p style="padding-left: 40px;">Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:</p> <p style="padding-left: 60px;">Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)</p> <p style="padding-left: 60px;">Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)</p> <p style="padding-left: 40px;">Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)</p> <p style="padding-left: 20px;">Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:</p> <p style="padding-left: 40px;">Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000001 (Create)</p>

Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
 Tag: Template-Attribute (0x4200008D), Type: Structure (0x80), Data:
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name
 Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:
 Tag: Name Value (0x42000050), Type: Text String (0x06), Data: Key1
 Tag: Name Type (0x4200004F), Type: Enumeration (0x04), Data: 0x00000001 (Uninterpreted text string)
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Algorithm
 Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000003 (AES)
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Length
 Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x00000080 (128)
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Usage Mask
 Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x00000004 (Encrypt)

42000073800000014742000072800000003042000065800000001A4200006601000000400000000420000670100000004
 000000624200000D010000000400000001420000F8000000105420000570400000004000000014200007480000000EF42
 0000520400000004000000024200008D800000000D94200000880000000304200000A06000000044E616D654200000B8000
 00001A4200005006000000044B6579314200004F04000000040000000142000008800000002D4200000A06000000174372
 7970746F6772617068696320416C676F726974686D4200000B04000000040000000342000008800000002A4200000A0600
 00001443727970746F67726170686963204C656E6774684200000B01000000040000008042000008800000002E4200000A
 060000001843727970746F67726170686963205573616765204D61736B4200000B010000000400000004

Out: objectType = '00000002', uuidKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0E9B (Wed Jan 14 17:12:43 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000001 (Create)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9

4200007680000000B04200007580000000041420000658000000001A4200006601000000400000000420000670100000004
 0000006242000008E080000000800000000496E0E9B4200000D010000000400000001420000F800000005D420000570400
 000004000000014200007A0400000004000000042000077800000003A420000520400000004000000024200008F060000
 002431663136356436352D636262642D346264362D393836372D383065306233393061636639

1	Client A:
---	-----------

Add attribute [batch]

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

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)
Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 26B1810D37F208ED
Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9
Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Activation Date
Tag: Attribute Value (0x4200000B), Type: Date-Time (0x08), Data: 0x0000000000000002 (Thu Jan 01 01:00:02 CET 1970)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)
Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: A87E7D9F6EC63107
Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9
Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Protect Stop Date
Tag: Attribute Value (0x4200000B), Type: Date-Time (0x08), Data: 0x00000000496E1153 (Wed Jan 14 17:22:43 CET 2009)

42000073800000015942000072800000003042000065800000001A4200006601000000400000000420000670100000004
000000624200000D0100000004000000024200000F80000000864200005704000000040000000D42000090070000000826
B1810D37F208ED42000074800000005F4200008F060000002431663136356436352D636262642D346264362D393836372D
3830653062333930616366394200000880000000294200000A060000000F41637469766174696F6E20446174654200000B
0800000080000000000000024200000F80000000884200005704000000040000000D420000900700000008A87E7D9F6E
C631074200007480000000614200008F060000002431663136356436352D636262642D346264362D393836372D38306530
623339306163663942000008800000002B4200000A060000001150726F746563742053746F7020446174654200000B0800
00000800000000496E1153

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

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0EFC (Wed Jan 14 17:12:44 CET 2009)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000002 (2)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

- Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)
- Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: 26B1810D37F208ED
- Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
- Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 - Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9
 - Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 - Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Activation Date
 - Tag: Attribute Value (0x4200000B), Type: Date-Time (0x08), Data: 0x0000000000000002 (Thu Jan 01 01:00:02 CET 1970)
- Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 - Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)
 - Tag: Unique Message ID (0x42000090), Type: Octet String (0x07), Data: A87E7D9F6EC63107
 - Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 - Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 - Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9
 - Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 - Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Protect Stop Date
 - Tag: Attribute Value (0x4200000B), Type: Date-Time (0x08), Data: 0x00000000496E1153 (Wed Jan 14 17:22:43 CET 2009)

420000768000000184420000758000000004142000065800000001A42000066010000000400000000420000670100000004
 000000624200008E080000000800000000496E0EFC4200000D0100000004000000024200000F8000000093420000570400
 00000400000000D42000090070000000826B1810D37F208ED4200007A04000000040000000042000077800000005F420000
 8F060000002431663136356436352D636262642D346264362D393836372D38306530623339306163663942000008800000
 00294200000A060000000F41637469766174696F6E20446174654200000B080000000800000000000000000024200000F8000
 0000954200005704000000040000000D420000900700000008A87E7D9F6EC631074200007A040000000400000000420000
 7780000000614200008F060000002431663136356436352D636262642D346264362D393836372D38306530623339306163
 663942000008800000002B4200000A060000001150726F746563742053746F7020446174654200000B0800000008000000
 00496E1153

2	<p>Client A:</p> <p>Add Attribute</p> <p>In: uuidKey, attribute={ UsageLimits={ UsageLimitsTotalBytes='1000' } }</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data:</p> <ul style="list-style-type: none"> Tag: Request Header (0x42000072), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0) Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98) Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1) Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute) Tag: Request Payload (0x42000074), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9 Tag: Attribute (0x42000008), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Usage Limits Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data: <ul style="list-style-type: none"> Tag: Usage Limits Total Bytes (0x42000094), Type: Big Integer (0x03), Data: 03E8 (1000)
---	--

4200007380000000E742000072800000003042000065800000001A42000066010000000400000000420000670100000004
000000624200000D01000000040000000014200000F800000000754200005704000000040000000D42000074800000005F42
00008F060000002431663136356436352D636262642D346264362D393836372D3830653062333930616366394200000880
000000294200000A0600000000C5573616765204C696D6974734200000B8000000000B42000094030000000203E8

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

Tag: Response Header (0x42000075), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0EFC (Wed Jan 14 17:12:44 CET 2009)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)

Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Usage Limits

Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:

Tag: Usage Limits Total Bytes (0x42000094), Type: Big Integer (0x03), Data: 03E8 (1000)

Tag: Usage Limits Byte Count (0x42000092), Type: Big Integer (0x03), Data: 03E8 (1000)

4200007680000000E04200007580000000041420000658000000001A42000066010000000400000000420000670100000004
000000624200008E0800000008000000000496E0EFC4200000D0100000004000000014200000F800000008D420000570400
0000040000000D4200007A04000000040000000042000077800000006A4200008F060000002431663136356436352D6362
62642D346264362D393836372D383065306233393061636639420000088000000034420000A060000000C557361676520
4C696D6974734200000B800000001642000094030000000203E842000092030000000203E8

3

Client B:

Locate (symmetric key by name)

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:

Tag: Request Header (0x42000072), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)

Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Type

Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)

Tag: Attribute (0x42000008), Type: Structure (0x80), Data:

Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name

Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:
Tag: Name Value (0x42000050), Type: Text String (0x06), Data: Key1
Tag: Name Type (0x4200004F), Type: Enumeration (0x04), Data: 0x00000001 (Uninterpreted text string)

4200007380000000BB42000072800000003042000065800000001A42000066010000000400000000420000670100000004
000000624200000D010000000400000001420000F80000000794200005704000000040000000842000074800000006342
0000088000000021420000A060000000B4F626A65637420547970654200000B040000000400000002420000880000000
304200000A06000000044E616D654200000B800000001A4200005006000000044B6579314200004F040000000400000001

Out: uuidKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0EFD (Wed Jan 14 17:12:45 CET 2009)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)
Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9

4200007680000000A3420000758000000004142000065800000001A42000066010000000400000000420000670100000004
000000624200008E080000000800000000496E0EFD4200000D010000000400000001420000F8000000050420000570400
00004000000084200007A04000000040000000042000077800000002D4200008F060000002431663136356436352D6362
62642D346264362D393836372D383065306233393061636639

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9

42000073800000008542000072800000003042000065800000001A42000066010000000400000000420000670100000004
000000624200000D010000000400000001420000F80000000434200005704000000040000000A42000074800000002D42
00008F060000002431663136356436352D636262642D346264362D393836372D383065306233393061636639

Out: objectType = '00000002', uuidKey, symmetricKey

```

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
  Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
    Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
      Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
    Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0EFD (Wed Jan 14 17:12:45 CET 2009)
    Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
  Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
    Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
    Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
      Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9
      Tag: Symmetric Key (0x4200008A), Type: Structure (0x80), Data:
        Tag: Key Block (0x4200003C), Type: Structure (0x80), Data:
          Tag: Key Value Type (0x42000040), Type: Enumeration (0x04), Data: 0x00000001
          Tag: Key Value (0x4200003F), Type: Structure (0x80), Data:
            Tag: Key Material (0x4200003D), Type: Octet String (0x07), Data:
17565C68ADC26DB563319588CAEB473A
            Tag: Cryptographic Algorithm (0x42000025), Type: Enumeration (0x04), Data: 0x00000003 (AES)
            Tag: Cryptographic Length (0x42000026), Type: Integer (0x01), Data: 0x00000080 (128)

```

```

42000076800000010B420000758000000004142000065800000001A42000066010000000400000000420000670100000004
000000624200008E080000000800000000496E0EFD4200000D010000000400000001420000F80000000B8420000570400
0000040000000A4200007A040000000400000000420000778000000095420000520400000004000000024200008F060000
002431663136356436352D636262642D346264362D393836372D3830653062333930616366394200008A800000000524200
003C8000000049420000400400000004000000014200003F800000000194200003D070000001017565C68ADC26DB5633195
88CAEB473A4200002504000000040000000342000026010000000400000080

```

5

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

```

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
  Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
    Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
      Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
    Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
  Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
    Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000011 (Get Usage Allocation)
    Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
      Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9
      Tag: Usage Limits Byte Count (0x42000092), Type: Big Integer (0x03), Data: 01F4 (500)

```

```

42000073800000009042000072800000003042000065800000001A42000066010000000400000000420000670100000004

```

00000062420000D010000000400000001420000F800000004E4200005704000000040000001142000074800000003842
00008F060000002431663136356436352D636262642D346264362D393836372D3830653062333930616366394200009203
0000000201F4

Out: uuidKey, UsageLimitsByteCount='500'

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0EFD (Wed Jan 14
17:12:45 CET 2009)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000011 (Get Usage Allocation)
Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-
9867-80e0b390acf9
Tag: Usage Limits Byte Count (0x42000092), Type: Big Integer (0x03), Data: 01F4 (500)

42000076800000000AE420000758000000004142000065800000001A42000066010000000400000000420000670100000004
000000624200008E0800000008000000000496E0EFD4200000D010000000400000001420000F800000005B420000570400
000004000000114200007A0400000004000000004200007780000000384200008F060000002431663136356436352D6362
62642D346264362D393836372D38306530623339306163663942000092030000000201F4

6

Client A:

Get usage allocation

In: uuidKey, UsageLimitsByteCount='500'

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000011 (Get Usage Allocation)
Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-
9867-80e0b390acf9
Tag: Usage Limits Byte Count (0x42000092), Type: Big Integer (0x03), Data: 01F4 (500)

420000738000000009042000072800000003042000065800000001A42000066010000000400000000420000670100000004
00000062420000D010000000400000001420000F800000004E4200005704000000040000001142000074800000003842
00008F060000002431663136356436352D636262642D346264362D393836372D3830653062333930616366394200009203
0000000201F4

Out: uuidKey, UsageLimitsByteCount='500'

```

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
  Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
    Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
      Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
    Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0EFD (Wed Jan 14 17:12:45 CET 2009)
    Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
  Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
    Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000011 (Get Usage Allocation)
    Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
      Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9
      Tag: Usage Limits Byte Count (0x42000092), Type: Big Integer (0x03), Data: 01F4 (500)

420000768000000000AE420000758000000004142000065800000001A42000066010000000400000000420000670100000004
00000624200008E080000000800000000496E0EFD420000D01000000040000001420000F800000005B420000570400
00004000000114200007A0400000004000000004200007780000000384200008F060000002431663136356436352D6362
62642D346264362D393836372D38306530623339306163663942000092030000000201F4

```

7

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

```

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
  Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
    Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
      Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
      Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
    Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
  Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
    Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
      Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
        Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Object Type
        Tag: Attribute Value (0x4200000B), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
      Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
        Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Name
        Tag: Attribute Value (0x4200000B), Type: Structure (0x80), Data:
          Tag: Name Value (0x42000050), Type: Text String (0x06), Data: Key1
          Tag: Name Type (0x4200004F), Type: Enumeration (0x04), Data: 0x00000001 (Uninterpreted text string)

420000738000000000BB42000072800000003042000065800000001A42000066010000000400000000420000670100000004
0000062420000D010000000400000001420000F8000000079420000570400000004000000842000074800000006342
0000880000000021420000A060000000B4F626A6563742054797065420000B040000000400000002420000880000000
30420000A06000000044E616D65420000B800000001A4200005006000000044B6579314200004F04000000040000001

```

Out: uuidKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0EFE (Wed Jan 14 17:12:46 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000008 (Locate)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9

4200007680000000A342000075800000004142000065800000001A42000066010000004000000042000067010000004
 000000624200008E080000000800000000496E0EFE420000D01000000400000001420000F8000000050420000570400
 000004000000084200007A0400000004000000042000077800000002D4200008F060000002431663136356436352D6362
 62642D346264362D393836372D383065306233393061636639

8

Client C:
Get (symmetric key)
In: uuidKey

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9

42000073800000008542000072800000003042000065800000001A42000066010000004000000042000067010000004
 00000062420000D01000000400000001420000F8000000043420000570400000040000000A42000074800000002D42
 00008F060000002431663136356436352D636262642D346264362D393836372D383065306233393061636639

Out: objectType = '00000002', uuidKey, symmetricKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0EFE (Wed Jan 14 17:12:46 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000A (Get)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9
 Tag: Symmetric Key (0x4200008A), Type: Structure (0x80), Data:
 Tag: Key Block (0x4200003C), Type: Structure (0x80), Data:
 Tag: Key Value Type (0x42000040), Type: Enumeration (0x04), Data: 0x00000001
 Tag: Key Value (0x4200003F), Type: Structure (0x80), Data:
 Tag: Key Material (0x4200003D), Type: Octet String (0x07), Data: 17565C68ADC26DB563319588CAEB473A
 Tag: Cryptographic Algorithm (0x42000025), Type: Enumeration (0x04), Data: 0x00000003 (AES)
 Tag: Cryptographic Length (0x42000026), Type: Integer (0x01), Data: 0x00000080 (128)

42000076800000010B420000758000000004142000065800000001A42000066010000000400000000420000670100000004
 000000624200008E080000000800000000496E0EFE420000D010000000400000001420000F80000000B8420000570400
 0000040000000A4200007A040000000400000000420000778000000095420000520400000004000000024200008F060000
 002431663136356436352D636262642D346264362D393836372D3830653062333930616366394200008A80000000524200
 003C8000000049420000400400000004000000014200003F80000000194200003D070000001017565C68ADC26DB5633195
 88CAEB473A4200002504000000040000000342000026010000000400000080

9

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000011 (Get Usage Allocation)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9
 Tag: Usage Limits Byte Count (0x42000092), Type: Big Integer (0x03), Data: 01F4 (500)

42000073800000009042000072800000003042000065800000001A42000066010000000400000000420000670100000004
 00000062420000D010000000400000001420000F800000004E4200005704000000040000001142000074800000003842
 00008F060000002431663136356436352D636262642D346264362D393836372D3830653062333930616366394200009203
 0000000201F4

Out: uuidKey, UsageLimitsByteCount='0'

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0EFE (Wed Jan 14 17:12:46 CET 2009)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000011 (Get Usage Allocation)

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)

Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9

Tag: Usage Limits Byte Count (0x42000092), Type: Big Integer (0x03), Data: 00 (0)

4200007680000000AD420000758000000004142000065800000001A4200006601000000040000000042000067010000000400000624200008E080000000800000000496E0EFE420000D010000000400000001420000F800000005A42000057040000004000000114200007A0400000004000000004200007780000000374200008F060000002431663136356436352D636262642D346264362D393836372D38306530623339306163663942000092030000000100

10

Client A:

Destroy (symmetric key)

In: uuidKey

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:

Tag: Request Header (0x42000072), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy)

Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9

42000073800000008542000072800000003042000065800000001A420000660100000004000000004200006701000000040000062420000D010000000400000001420000F8000000043420000570400000004000000142000074800000002D420000F0600000002431663136356436352D636262642D346264362D393836372D383065306233393061636639

Out: uuidKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

Tag: Response Header (0x42000075), Type: Structure (0x80), Data:

Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:

Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)

Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E0EFE (Wed Jan 14 17:12:46 CET 2009)

Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)

Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:

Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000014 (Destroy)

Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)

Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:

Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 1f165d65-cbbd-4bd6-9867-80e0b390acf9

```

4200007680000000A3420000758000000004142000065800000001A42000066010000000400000000420000670100000004
000000624200008E0800000008000000000496E0EFE420000D0100000004000000014200000F8000000050420000570400
000004000000144200007A04000000040000000042000077800000002D4200008F060000002431663136356436352D6362
62642D346264362D393836372D383065306233393061636639

```

6 Key Interchange, Key Exchange

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

This use-case tests the import of a foreign key.

Time	Request/Response messages
0	<p>Register (symmetric key) In: objectType = '00000002', CryptographicUsageMask='00000004', foreignSymmetricKey</p> <p>Tag: Request Message (0x42000073), Type: Structure (0x80), Data:</p> <p> Tag: Request Header (0x42000072), Type: Structure (0x80), Data:</p> <p> Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:</p> <p> Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)</p> <p> Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)</p> <p> Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)</p> <p> Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:</p> <p> Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000003 (Register)</p> <p> Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:</p> <p> Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)</p> <p> Tag: Template-Attribute (0x4200008D), Type: Structure (0x80), Data:</p> <p> Tag: Attribute (0x42000008), Type: Structure (0x80), Data:</p> <p> Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: Cryptographic Usage Mask</p> <p> Tag: Attribute Value (0x4200000B), Type: Integer (0x01), Data: 0x00000004 (Encrypt)</p> <p> Tag: Symmetric Key (0x4200008A), Type: Structure (0x80), Data:</p> <p> Tag: Key Block (0x4200003C), Type: Structure (0x80), Data:</p> <p> Tag: Key Value Type (0x42000040), Type: Enumeration (0x04), Data: 0x00000001</p> <p> Tag: Key Value (0x4200003F), Type: Structure (0x80), Data:</p> <p> Tag: Key Material (0x4200003D), Type: Octet String (0x07), Data: 0123456789ABCDEF0123456789ABCDEF</p> <p> Tag: Cryptographic Algorithm (0x42000025), Type: Enumeration (0x04), Data: 0x00000003 (AES)</p> <p> Tag: Cryptographic Length (0x42000026), Type: Integer (0x01), Data: 0x00000080 (128)</p> <p>42000073800000010042000072800000003042000065800000001A42000066010000000400000000420000670100000004 400000062420000D0100000004000000014200000F80000000BE420000570400000004000000034200007480000000A8 420000520400000004000000024200008D800000003742000008800000002E420000A060000001843727970746F67726 170686963205573616765204D61736B420000B0100000004000000044200008A80000000524200003C80000000494200 00400400000004000000014200003F80000000194200003D07000000100123456789ABCDEF0123456789ABCDEF4200002</p>

5040000004000000034200002601000000400000080

Out: objectType = '00000002', uuidKey

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E1037 (Wed Jan 14 17:17:59 CET 2009)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x00000003 (Register)
Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
Tag: Object Type (0x42000052), Type: Enumeration (0x04), Data: 0x00000002 (Symmetric Key)
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 945a00b0-b211-49e8-acfe-adc31c873695

4200007680000000B0420000758000000004142000065800000001A4200006601000000040000000042000067010000000
4000000624200008E080000000800000000496E1037420000D0100000004000000014200000F800000005D4200005704
00000004000000034200007A04000000040000000042000077800000003A420000520400000004000000024200008F060
000002439343561303062302D623231312D343965382D616366652D616463333163383733363935

1

Add attribute

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)
Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 945a00b0-b211-49e8-acfe-adc31c873695
Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-provider
Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: unknown

4200007380000000B142000072800000003042000065800000001A4200006601000000040000000042000067010000000
400000062420000D0100000004000000014200000F800000006F4200005704000000040000000D420000748000000059
4200008F060000002439343561303062302D623231312D343965382D616366652D6164633331633837333639354200000
88000000023420000A060000000A782D70726F7669646572420000B0600000007756E6B6E6F776E

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:

Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E1038 (Wed Jan 14 17:18:00 CET 2009)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000D (Add Attribute)
 Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)
 Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 945a00b0-b211-49e8-acfe-adc31c873695
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-provider
 Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: unknown

4200007680000000CF42000075800000004142000065800000001A420000660100000040000000420000670100000000
 4000000624200008E080000000800000000496E1038420000D01000000400000001420000F800000007C4200005704
 000000040000000D4200007A0400000004000000004200007780000000594200008F0600000002439343561303062302D6
 23231312D343965382D616366652D616463333163383733363935420000088000000023420000A060000000A782D7072
 6F7669646572420000B0600000007756E6B6E6F776E

2

Modify attribute

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

Tag: Request Message (0x42000073), Type: Structure (0x80), Data:
 Tag: Request Header (0x42000072), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)
 Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)
 Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)
 Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:
 Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000E (Modify Attribute)
 Tag: Request Payload (0x42000074), Type: Structure (0x80), Data:
 Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 945a00b0-b211-49e8-acfe-adc31c873695
 Tag: Attribute (0x42000008), Type: Structure (0x80), Data:
 Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-provider
 Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: third party

4200007380000000B542000072800000003042000065800000001A420000660100000040000000420000670100000000
 400000062420000D01000000400000001420000F8000000073420000570400000040000000E42000074800000005D
 4200008F060000002439343561303062302D623231312D343965382D616366652D6164633331633837333639354200000
 88000000027420000A060000000A782D70726F7669646572420000B060000000B7468697264207061727479

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

Tag: Response Message (0x42000076), Type: Structure (0x80), Data:
 Tag: Response Header (0x42000075), Type: Structure (0x80), Data:
 Tag: Protocol Version (0x42000065), Type: Structure (0x80), Data:
 Tag: Protocol Version Major (0x42000066), Type: Integer (0x01), Data: 0x00000000 (0)

<p>Tag: Protocol Version Minor (0x42000067), Type: Integer (0x01), Data: 0x00000062 (98)</p> <p>Tag: Time Stamp (0x4200008E), Type: Date-Time (0x08), Data: 0x00000000496E1038 (Wed Jan 14 17:18:00 CET 2009)</p> <p>Tag: Batch Count (0x4200000D), Type: Integer (0x01), Data: 0x00000001 (1)</p> <p>Tag: Batch Item (0x4200000F), Type: Structure (0x80), Data:</p> <p>Tag: Operation (0x42000057), Type: Enumeration (0x04), Data: 0x0000000E (Modify Attribute)</p> <p>Tag: Result Status (0x4200007A), Type: Enumeration (0x04), Data: 0x00000000 (Success)</p> <p>Tag: Response Payload (0x42000077), Type: Structure (0x80), Data:</p> <p>Tag: Unique Identifier (0x4200008F), Type: Text String (0x06), Data: 945a00b0-b211-49e8-acfe-adc31c873695</p> <p>Tag: Attribute (0x42000008), Type: Structure (0x80), Data:</p> <p>Tag: Attribute Name (0x4200000A), Type: Text String (0x06), Data: x-provider</p> <p>Tag: Attribute Value (0x4200000B), Type: Text String (0x06), Data: third party</p> <p>4200007680000000D342000075800000004142000065800000001A42000066010000000400000000420000670100000004000000624200008E080000000800000000496E10384200000D0100000004000000014200000F80000000804200005704000000040000000E4200007A0400000004000000042000077800000005D4200008F060000002439343561303062302D623231312D343965382D616366652D61646333316338373336393542000008800000000274200000A060000000A782D70726F76696465724200000B060000000B7468697264207061727479</p>
--

7 Vendor Extensions

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

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

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

Time	Client A
0	<p>Create (symmetric key)</p> <p>In: objectType='00000002', CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='00000012', MessageExtension={ VendorIdentification='Acme', CriticalityIndicator='false', VendorExtension={ tag='0x42014242', type='text string', value='na' } }</p> <p>Out: objectType='00000002', uuidKey</p>
1	<p>Destroy (symmetric key)</p> <p>In: uuidKey</p> <p>Out: uuidKey</p>

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

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

Time	Client A
0	<p>Create (symmetric key)</p> <p>In: objectType='00000002', CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='00000012', MessageExtension={ VendorIdentification='Acme', CriticalityIndicator='true', VendorExtension={ tag='0x42014242', type='text string', value='na' } }</p> <p>Out: Operation Failed, Feature Not Supported</p>

8 Asymmetric keys

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

8.1 Use-case: Create a Key Pair

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

Time	Client A
0	<p>Create Key Pair</p> <p>In: commonAttributes={ CryptographicAlgorithm='RSA', CryptographicLength='1024', CryptographicUsageMask='00000012' }, privateKeyAttributes={ Name={ NameValue='PrivateKey1', NameType='00000001' } }, publicKeyAttributes={ NameValue='PublicKey1', NameType='00000001' } }</p> <p>Out: uuidPrivateKey, uuidPublicKey</p>
1	<p>Locate (Public Key)</p> <p>In: attributes={ objectType='PublicKey', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } }</p> <p>Out: uuidPublicKey</p>
2	<p>Locate (Private Key)</p> <p>In: attributes={ objectType='PrivateKey', Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } }</p> <p>Out: uuidPrivateKey</p>

3	Destroy In: uuidPrivateKey Out: uuidPrivateKey
4	Destroy In: uuidPublicKey Out: uuidPublicKey

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

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

Time	Client A
0	Register (Private Key) In: objectType='00000004', CryptographicUsageMask='00000012', foreignPrivateKey Out: uuidPrivateKey
1	Register (Public Key) In: objectType='00000004', CryptographicUsageMask='00000012', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey }, foreignPublicKey Out: uuidPublicKey
2	Add attribute In: uuidPrivateKey, attribute={ Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } } Out: uuidPrivateKey, attribute={ Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } }
3	Locate (Public Key) In: attributes={ objectType='PublicKey', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } } Out: uuidPublicKey
4	Locate (Private Key) In: attributes={ objectType='PrivateKey', Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } } Out: uuidPrivateKey
5	Destroy In: uuidPrivateKey Out: uuidPrivateKey
6	Destroy In: uuidPublicKey Out: uuidPublicKey

9 Key Roll-over

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

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

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

Time	Client A
0	Create (symmetric key) In: objectType='00000002', CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='00000012', Name={ NameValue='rekeyKey', NameType='00000001' } Out: objectType='00000002', uuidKey
1	Locate In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Out: uuidKey
2	Rekey In: uuidKey Out: uuidNewKey
3	Locate In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Out: uuidNewKey
4	Get Attribute In: uuidKey, attributeName={'Name'} Out: Operation Failed, Item Not Found
5	Get (symmetric key) In: uuidKey Out: objectType = '00000002', uuidKey, symmetricKey
6	Destroy In: uuidKey Out: uuidKey
7	Destroy In: uuidNewKey

Out: uuidNewKey

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

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

Time	Client A
0	Create (symmetric key) In: objectType='00000002', CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='00000012' Out: objectType='00000002', uuidKey
1	Add Activation Date, Deactivation Date attributes based on Timestamp in previous response (batch) In: uuidKey, attribute={ ActivationDate=' <Timestamp in previous response - 365 days>' } In: uuidKey, attribute={ DeactivationDate=' <Timestamp in previous response + 2 minutes>' } Out: uuidKey, attribute={ ActivationDate=' <Timestamp in previous response - 1 year>' } Out: uuidKey, attribute={ DeactivationDate=' <Timestamp in previous response + 2 minutes>' }
2	Get Attribute * Repeated until state changes to Deactivated In: uuidKey, attributeName={'State'} Out: uuidKey, attribute={ State='Active' }
3	Get Attribute In: uuidKey, attributeName={'State'} Out: uuidKey, attribute={ State='Deactive' }
4	Rekey In: uuidKey, attribute={ offset='018B8200' (300 days)} Out: uuidNewKey
5	Get Attribute In: uuidNewKey, attributeName={' ActivationDate', 'DeactivationDate' } Out: uuidNewKey, attribute={ ActivationDate=' <Value of ActivationTime in existing key + 300 days>', DeactivationDate=' <Value of DeactivationDate of existing key + 300 days>' }
6	Get Attribute In: uuidNewKey, attributeName={'State'} Out: uuidNewKey, attribute={ State='Active' }

7	Destroy In: uuidKey Out: uuidKey
8	Destroy In: uuidNewKey Out: uuidNewKey

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

Create a new symmetric key with the *Activation Date* in the past. Do a Get Attribute operation on the State attribute to verify the key is “Active”. Then revoke the key as compromised, verify that the state has changed to “Compromised”. Create a replacement key using Re-key with the offset set to ‘0’ to indicate that the times will be copied from the existing key. Do a Get Attribute operation to verify that the state of the new key is “Active”. To clean up, both keys are deleted.

Time	Client A
0	Create (symmetric key) In: objectType='00000002', CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='00000012', Name={ NameValue='rekeyKey', NameType='00000001' }, ActivationDate='2' Out: objectType='00000002', uuidKey
1	Get Attribute In: uuidKey, attributeName={'State'} Out: uuidKey, attribute={ State='Active' }
2	Revoke (symmetric key as compromised) In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceDate='6' Out: uuidKey
3	Get Attribute In: uuidKey, attributeName={'State'} Out: uuidKey, attribute={ State='Compromised' }
4	Rekey In: uuidKey, offset='0' Out: uuidNewKey
5	Get Attribute In: uuidNewKey, attributeName={'State'} Out: uuidNewKey, attribute={ State='Active' }
6	Destroy In: uuidKey Out: uuidKey

7	Destroy In: uuidNewKey Out: uuidNewKey
---	--

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

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

Time	Client A
0	Create (symmetric key) In: objectType='00000002', CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='00000012', Name={ NameValue='rekeyKey', NameType='00000001' } Out: objectType='00000002', uuidKey
1	Locate In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Out: uuidKey
2	Rekey In: uuidKey, attributes={ ActivationDate='0000000043B7B630', ProcessStartDate='0000000043B7B630', ProtectStopDate='000000005E0C7BB0', DeactivationDate='000000005E0C7BB0' } Out: uuidNewKey
3	Get Attribute In: uuidKey, attributeName={'Name'} Out: Operation Failed, Item Not Found
4	Get Attribute In: uuidKey, attributeName={ 'ActivationDate', 'ProcessStartDate', 'ProtectStopDate', 'DeactivationDate' } Out: uuidKey, attribute={ ActivationDate='0000000043B7B630', ProcessStartDate='0000000043B7B630', ProtectStopDate='000000005E0C7BB0', DeactivationDate='000000005E0C7BB0' }
5	Locate In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Out: uuidNewKey
6	Destroy In: uuidKey Out: uuidKey
7	Destroy In: uuidNewKey Out: uuidNewKey

9.5 Use-case: Obtain Lease for Expired Key

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

Time	Client A	Client B
0	Create (symmetric key) In: objectType='00000002', CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='00000012', Name={ NameValue=' rekeyKey', NameType='00000001' }, ActivationDate='2' Out: objectType='00000002', uuidKey	
1	Get (symmetric key) In: uuidKey Out: objectType = '00000002', uuidKey, symmetricKey	
2	Obtain Lease In: uuidKey Out: uuidKey, leaseTime, lastChangeDate	
3		Revoke (symmetric key as compromised) In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceDate='6' Out: uuidKey
4		Rekey In: uuidKey, offset='0' Out: uuidNewKey
5	Obtain Lease In: uuidKey Out: Operation Failed, Permission Denied	
6	Locate (symmetric key) In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Out: uuidNewKey	
7	Get (symmetric key) In: uuidNewKey Out: objectType = '00000002', uuidNewKey,	

	newSymmetricKey	
8	Obtain Lease In: uuidNewKey Out: uuidNewKey, leaseTime, lastChangeDate	
9	Destroy In: uuidKey Out: uuidKey	
10	Destroy In: uuidNewKey Out: uuidNewKey	

10 Archival

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

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

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

Time	Client A
0	Create (symmetric key) In: objectType='00000002', CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='00000012', Name={ NameValue='archiveKey', NameType='00000001' } Out: objectType='00000002', uuidKey
1	Locate In: attributes={ Name={ NameValue='archiveKey', NameType='00000001' } } Out: uuidKey
2	Get (symmetric key) In: uuidKey Out: objectType = '00000002', uuidKey, symmetricKey
3	Archive In: uuidKey, asynchronousIndicator='true' Out: asynchronousCorrelationValue

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

A. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Original Authors of the initial contribution:

David Babcock, HP
Joseph Birr-Pixton, Thales/nCipher
Mathias Björkqvist, IBM (editor)
John Clark, HP
Stan Feather, HP
Jon Geater, nCipher
Bob Griffin, EMC
Robert Haas, IBM
Jack Harwood, EMC
Vlad Libershteyn, HP
Mark Lin, EMC/RSA
Brian Metzger, HP
Madhav Mutalik, EMC/RSA
Anthony Nadalin, IBM
René Pawlitzek, IBM (editor)
Bruce Rich, IBM
Parameswaran Seshan, EMC/RSA
John Tattan, EMC

Participants:

[TBD](#)

B. Revision History

Revision	Date	Editor	Changes Made
ed-0.98	2009-04-28	Mathias Björkqvist	Initial conversion of input document to OASIS format.