Key Management Interoperability Protocol Use Cases Version 1.0

Committee Draft 06 / Public Review 02

12 November 2009

Specification URIs:
This Version:
http://docs.oasis-open.org/kmip/usecases/v1.0/cd06/kmip-usecases-1.0-cd-06.html
http://docs.oasis-open.org/kmip/usecases/v1.0/cd06/kmip-usecases-1.0-cd-06.doc (Authoritative)
http://docs.oasis-open.org/kmip/usecases/v1.0/cd06/kmip-usecases-1.0-cd-06.pdf

Previous Version:

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

Technical Committee:
OASIS Key Management Interoperability Protocol (KMIP) TC

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

Editor(s):
Mathias Björkqvist, IBM <mbj@zurich.ibm.com>
René Pawlitzek, IBM <rpa@zurich.ibm.com>

Related work:
This specification replaces or supersedes:

- None

This specification is related to:

- Key Management Interoperability Protocol Specification Version 1.0, http://docs.oasis-open.org/kmip/spec/v1.0/
- Key Management Interoperability Protocol Profiles Version 1.0, http://docs.oasis-open.org/kmip/profiles/v1.0/
- Key Management Interoperability Protocol Usage Guide Version 1.0, http://docs.oasis-open.org/kmip/ug/v1.0/

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

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

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

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/.

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

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

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

1 Introduction

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

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

1.1 Normative References

[KMIP-Spec] OASIS Draft, *Key Management Interoperability Specification v1.0,* Committee Draft, November 2009.

[KMIP-Prof] OASIS Draft, *Key Management Interoperability Protocol Profiles v1,0,* Committee Draft, November 2009.

2 Message exchange

The message exchange between clients and the server to test the following use-case scenarios is performed with TTLV encoding over the http transport. This is to facilitate debugging and to focus on KMIP-specific issues instead of potential secure transport setup problems.

3 Centralized Management

3.1 Basic functionality

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

3.1.1 Use-case: Create / Destroy

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

Time	Request/Response messages
0	Create (symmetric key)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

In: objectType=’00000002’ (Symmetric Key), attributes={ CryptographicAlgorithm=’00000003’ (AES), CryptographicLength=’128’, CryptographicUsageMask=‘0000000C’ }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic
Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt,
Decrypt)
```

```
42007801000001204200770100000038420069010000002042006A020000000400000001000000042006B0200000004
000000000000000042000D020000000400000001000000042000F01000000D842005C05000000040000000100000000
42007901000000C042005705000000040000000200000000420091010000000A8420008010000003042000A0700000017
43727970746F6772617068696320416C676F726974686D0042000B050000000400000003000000042000801000000030
42000A0700000014437279707 46F67726170686963204C656E6774680000000042000B020000000400000008000000000
42000801000000304 2000A0700000018437279707 46F6772617068696320557361676520 4D61736B42000B0200000004
0000000C00000000
```

Out: objectType=’00000002’, uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C2 (Thu Nov 12
11:47:30 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
```


Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fc8833de-70d2-4ece-b063-fede3a3c59fe 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000004200 6B0200000004000000000000000042009209000000080000000004AFBE7C242000D020000000400000001000000004200 0F0100000068420005C050000000400000001000000004200 7F0500000004000000000000000042007C0100000040420057050000000400000002000000004200 9407000000246663383833336465 2D373064322D346563652D623036332D6665646533613363353966650000000 0
1	Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fc8833de-70d2-4ece-b063-fede3a3c59fe 42007801000000904200770100000038420069010000002042006A020000000400000001000000004200 6B0200000004000000000000000042000D020000000400000001000000004200 0F0100000048420005C050000000400000001400000000420079010000003042009407000000246663383833336465 2D373064322D346563652D623036332D6665646533613363353966650000000 0 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C3 (Thu Nov 12 11:47:31 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fc8833de-70d2-4ece-b063-fede3a3c59fe 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B0200000004000000000000000042009209000000080000000004AFBE7C342000D020000000400000001000000004200 0F0100000058420005C050000000400000001400000000420079F0500000004000000000000000042007C0100000030420094070000002466633838333364652D373064322D346563652D623036332D6665646533613363353966650000000 0

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

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

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

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

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000006 (Template)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Application Specific
Information
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Application Namespace (0x420003), Type: Text String (0x07), Data: ssl
            Tag: Application Data (0x420002), Type: Text String (0x07), Data: www.example.com
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-Purpose
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: demonstration
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: Template1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)


42007801000001C0420077010000003842006901000002042006A020000000400000001000000042006B02000000040
000000000000000042000D020000000400000001000000042000F01000001784200501000000284200A070000000C4F6
0079010000016042005705000000040000000600000000420091010000014842000801000000284200A070000000C4F6
26A6563742047726F757000000000042000B07000000647726F75703100004200080100000058420 00A07000000204170
706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000B0100000028420003070000000373736
C0000000000420002070000000F7777772E6578616D706C652E636F6D0042000801000000304200 0A0700000013436F6E
```


Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	7461637420496E666F726D6174696F6E00000000042000B07000000034A6F650000000000420008010000003042000A0700000009782D507572706F7365000000000000042000B070000000D64656D6F6E7374726174696F6E00000042000801000000404200A07000000044E616D650000000042000B0100000028420055070000000954656D706C617465310000000000000042005405000000040000000100000000 Out: uuidTemplate Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C4 (Thu Nov 12 11:47:32 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a6ebbb6f-4c54-4bbb-ad29-be6bad4ecad5 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBE7C442000D020000000400000001000000042000F010000005842005C05000000040000000300000000042007F050000000400000000000000042007C0100000030420094070000002461366562626236662D346335342D346262622D616432392D626536626164346563616435000000000
1	Create (symmetric key using template) In: objectType=’00000002’, template={ NameValue=’Template1’, NameType=’00000001’ }, attributes={ CryptographicAlgorithm=’AES’, CryptographicLength=’128’, CryptographicUsageMask=‘0000000C’ } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Name (0x420053), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Template1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt) 42007801000001504200770100000038420069010000002042006A020000000400000001000000004200 6B02000000040000000000000004200 0D020000000400000001000000004200 0F01000001084200 5C05000000040000000100000000420 0790100000 0F042005705000000040000000200000000420091010000 00D84200530100000028420055070000 0009546 56D706C6174653100000000000000042005405000000040000000100000000420008010000003042000A07000000174372 7970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000 A0700000014437279707 46F6772617068696320 4C656E6774680000000042000B020000000400000080000000004200 08 0100000030420 00A0700000018437279707 46F6772617068696320557361676520 4D61736B42000B020000000400000000 C00000000 Out: objectType='00000002', uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C5 (Thu Nov 12 11:47:33 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-2fa6ea1d747a 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000004200 6B02000000040000000000000004200920900000008000000004AFBE7C542000D020000000400000001000000004200 0F010000006842 005C05000000040000000100000000420 07F05000000040000000000000000042007C0100000040420057050000000400000000200000000420094070000002436316231303631342D643862352D343666392D386431372D32666136656131643734376100000000
2	Get attributes In: uuidKey, attributeNames={'ObjectGroup', 'ApplicationSpecificInformation', 'ContactInformation', 'x-Purpose'} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-2fa6ea1d747a

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

```
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Application Specific
Information
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-Purpose


420078010000010842007701000000384200690100000020420 06A020000000400000001000000042006B02000000040
000000000000000042000D020000000400000001000000042000F01000000C042005C050000000400000000B0000000042
007901000000A842009407000000243631623130363134 2D643862352D343666392D386431372D3266613665613164373
437610000000042000A070000000C4F626A6563742047726F757000000000042000A0700000020417070 6C69636174696F
6E20537065636966696320496E666F726D6174696F6E42000A0700000013436F6E7461637420496E666F726D6174696F6
E000000000042000A0700000009782D507572706F736500000000000000
```

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

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C6 (Thu Nov 12
11:47:34 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-
2fa6ea1d747a
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Application Specific
Information
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Application Namespace (0x420003), Type: Text String (0x07), Data: ssl
          Tag: Application Data (0x420002), Type: Text String (0x07), Data: www.example.com
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-Purpose
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: demonstration


42007B01000001B042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040
000000000000000420092090000000800000000 4AFBE7C642000D020000000400000001000000042000F010000015842
005C050000000400000000B0000000042007F050000000400000000000000000042007C0100000130420094070000002436 3
16231303631342D643862352D343666392D386431372D3266613665613164373437610000000042000801000000284200
0A070000000C4F626A6563742047726F757000000000042000B070000000647726F75703100004200080100000058420000
A0700000020417070 6C69636174696F6E20537065636966696320496E666F726D6174696F6E42000B0100000028420003
070000000373736C000000000042000207000000 0F7777772E6578616D706C652E636F6D0042000801000000304200 0A0
700000013436F6E7461637420496E666F726D6174696F6E000000000042000B07000000034A6F650000000000042000801
```


Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	0000003042000A0700000009782D507572706F7365000000000000042000B070000000D64656D6F6E7374726174696F6E000000
3	Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-2fa6ea1d747a 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002436316231303631342D643862352D343666392D386431372D3266613665613164373437610000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C6 (Thu Nov 12 11:47:34 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-2fa6ea1d747a 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000008000000004AFBE7C642000D020000000400000001000000042000F010000005842005C050000000400000014000000042007F050000000400000000000000000042007C0100000030420094070000002436316231303631342D643862352D343666392D386431372D32666136656131643734376100000000
4	Destroy (template) In: uuidTemplate Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a6ebbb6f-4c54-4bbb-ad29-be6bad4ecad5 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002461366562626236662D346335342D346262622D616432392D6265366261643465636164350000000 Out: uuidTemplate Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C6 (Thu Nov 12 11:47:34 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a6ebbb6f-4c54-4bbb-ad29-be6bad4ecad5 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000008000000004AFBE7C642000D020000000400000001000000042000F010000005842005C050000000400000014000000004200 7F050000000400000000000000000042007C0100000030420094070000002461366562626236662D346335342D346262622D616432392D6265366261643465636164350000000

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

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

Time	Request/Response messages
0	Create (symmetric key) In: objectType = ‘00000002’, attributes={ Name={ NameValue=‘Key1’, NameType=’00000001’ }, CryptographicAlgorithm=’DES’, CryptographicLength=’56’, CryptographicUsageMask=‘0000000C’, ContactInformation=’Joe’ }

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000001 (DES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000038 (56)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt,
Decrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe


42007801000001984200770100000038420069010000002042006A020000000400000001000000004200
0000000000000042000D020000000400000001000000042000F010000015042005C050000000400000001000000042
00790100000138420057050000000400000002000000004200910100000120420008010000003842000A07000000044E6
16D650000000042000B01000000204200550700000044B65793100000000420054050000000400000001000000004200
08010000003042000A0700000017437279707 46F6772617068696320416C676F726974686D0042000B050000000400000
0010000000042000801000000 3042000A0700000014437279707 46F6772617068696320 4C656E6774680000000042000B
020000000400000038000000004200080100000030 42000A0700000018437279707 46F6772617068696320 55736167652
04D61736B42000B020000000400000000C000000004200080100000030 42000A0700000013436F6E7461637420496E666F
726D6174696F6E000000000042000B07000000034A6F650000000000
```

Out: objectType = ‘00000002’, uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C7 (Thu Nov 12
11:47:35 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
```


Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBE7C742000D020000000400000001000000042000F010000006842005C05000000040000000100000000042007F05000000040000000000000000042007C0100000040420057050000000400000002009407000000243165643238656135 2D326233312D343134352D626366322D33366430373536643338393000000000
1	Locate (symmetric key) In: attributes={ objectType = ‘00000002’, Name={ Name=‘Key1’, NameType=’00000001’} } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007801000000D042007701000000384200690100000020420 06A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000008842005C05000000040000000800000000420079010000007042000801000000284200 0A070000000B4F626A6563742054797065000000000042000B0500000004000000020000000042000801000000384200 0A07000000044E616D6500000000420 00B0100000020420055070000000044B6579310000000042005405000000040000000100000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C8 (Thu Nov 12 11:47:36 CET 2009)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBE7C842000D020000000400000001000000042000F010000005842005C05000000040000000800000042007F050000000400000000000000042007C0100000030420094070000002431656432386561352D326233312D343134352D626366322D333664303735366433383930000000000
2	Get (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890 420078010000009042007701000000384200690100000020420 06A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000004842005C05000000040000000A000000004200790100000030420094070000002431656432386561352D326233312D343134352D626366322D3336643037353664333383930000000000 Out: objectType = ‘00000002’, uuidKey, symmetricKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C8 (Thu Nov 12 11:47:36 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890 Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data:

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 4564A76DF1A77662 Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000001 (DES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000038 (56) 42007B01000011842007A0100000048420069010000002042006A020000000400000001000000042006B02000000040 00000000000000042009209000000080000000004AFBE7C842000D020000000400000001000000042000F01000000C042 005C0500000004000000A0000000042007F0500000004000000000000000042007C0100000098420057050000000400 0000200000000420094070000002431656432386561352D326233312D343134352D626366322D33366430373536643338 39300000000042008F0100000050420040010000004842004205000000040000000100000000420045010000001042004 308000000084564A76DF1A7766242002805000000040000001000000042002A020000004000003800000000
3	Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890 420078010000009042007701000000384200690100000020420 06A020000000400000001000000042006B02000000040 00000000000000042000D020000000400000001000000042000F010000004842005C050000000400000014000000004 2 00790100000030420094070000002431656432386561352D326233312D343134352D626366322D33366430373536643338 3393000000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C8 (Thu Nov 12 11:47:36 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040 00000000000000042009209000000080000000004AFBE7C842000D020000000400000001000000042000F010000005842

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002431656432386561352D326233312D343134352D626366322D333664303735366433383930000000000
4	Locate In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Unique Identifier Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-36d0756d3890 42007801000000B84200770100000038420069010000002042006A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000007042005C050000000400000008000000042007901000000584200080100000050420 00A0700000011556E697175652049646 56E7469666965720000000000000420 00B0700000024316564323865613 52D326233312D343134352D626366322D333664303735366433383930000000000 Out: <empty response payload> Tag: Response Message (0x420078), Type: Structure (0x01), Data: Tag: Response Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420067), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x420068), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x420069), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x42008F), Type: Date-Time (0x09), Data: 0x000000004AC07323 (Mon Sep 28 10:26:11 CEST 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005A), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007C), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x420079), Type: Structure (0x01), Data: null 42007B010000008042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBE7C842000D020000000400000001000000042000F010000002842005C0500000004000000080000000042007F0500000004000000000000000042007C0100000000

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

This use-case has two clients performing operations on the same key. The first client initially registers a template and creates a symmetric key using that template. The second client then does a batched Locate and Get using the ID Placeholder to retrieve the key. The second client thereafter performs a number of operations on the key (Get Attribute List, Get Attribute, Add Attribute, Modify Attribute and Delete

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

Attribute), before the first client finally destroys the key and the template. The first client also tries to Get the key and the template after they have been destroyed, but the Get operation fails in both cases.

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

Time	Request/Response messages
0	Client A: Register (template) In: objectType='00000007', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', Name={ NameValue='Template1', NameType='00000001' },} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000006 (Template) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Template1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007801000001304200770100000038420069010000002042006A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F01000000E842005C050000000400000003000000004200790100000D042005705000000040000000600000000420091010000000B84200080100000030420000A0700000017437279707 46F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000A07000000144372797074 6F6772617068696320416C656E6774680000000042000B020000000400000080000000004200080100000042000A07000000044E616D650000000042000B0100000028420055070000000954656D706C6174653100000000000042005405000000040000000100000000 Out: uuidTemplate

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

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

```
42007B01000000B042007A01000000484200690100000020420 06A020000000400000001000000004200 6B02000000040
0000000000000004200920900000008000000004AFBED2142000D020000000400000001000000004200 0F010000005842
005C050000000400000003000000004200 7F050000000400000000000000004200 7C010000003042009407000000243 43
56438363239612D396164312D343162332D396430392D393431663261353935646133000000000
```

1

Client A:

Create (symmetric key using template)

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

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Name (0x420053), Type: Structure (0x01), Data:
          Tag: Name Value (0x420055), Type: Text String (0x07), Data: Template1
          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt)
```


Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Foo 420078010000015842007701000000384200690100000020420 06A020000000400000001000000004200 6B02000000040 00000000000000042000D020000000400000001000000004200 0F01000001104200 5C0500000004000000010000000042 007901000000F84200570500000004000000020000000420091010000000E0420053010000002842005507000000095 46 56D706C617465310000000000000042005405000000040000000100000000420008010000003842000A07000000044E61 6D650000000042000B0100000020420055070000000044B65793100000000420054050000000400000001000000004200 0801000003042000A0700000018437279707 46F6772617068696320557361676520 4D61736B42000B0200000004000000 040000000042000801000000304200 0A0700000013436F6E7461637420496E666F726D6174696F6E00000000042000B0 700000003466F6F0000000000 Out: objectType='00000002', uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED23 (Thu Nov 12 12:10:27 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 42007B01000000C042007A01000000484200690100000020420 06A020000000400000001000000004200 6B02000000040 00000000000000004200920900000008000000004AFBED2342000D020000000400000001000000004200 0F010000006842 005C0500000004000000010000000042007F0500000004000000000000000042007C0100000040420057050000000400 0000200000000420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961 653300000000
2	Client B: Locate and Get (symmetric key by name) In (header): batchOrderOption='TRUE' In: attributes={ objectType = '00000002', Name={ Name='Key1', NameType='00000001'} } In: <empty Get payload> Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

```
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 0E9E1875336E415E
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric
Key)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: CFEF21DDDF1CF5E3
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data: null


420078010000012042007701000000484200690100000020420 06A020000000400000001000000004200 6B02000000040
000000000000000420010060000000800000000000000142000D020000000400000002000000004200 0F010000009842
005C050000000400000008000000004200930800000080E9E1875336E415E42007901000000704200080100000028420
00A070000000B4F626A6563742054797065000000000042000B050000000400000002000000004200080100000038420 0
0A07000000044E616D650000000042000B0100000020420055070000000 44B6579310000000042005405000000040000 0
0010000000042000F0100000028420 05C0500000004000000 0A000000042009308000000008CFEF21DDDF1CF5E3420079
0100000000
```

Out: uuidKey

Out: objectType='00000002', uuidKey, symmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED24 (Thu Nov 12
12:10:28 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 0E9E1875336E415E
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-
8d1c3bbf9ae3
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: CFEF21DDDF1CF5E3
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-
8d1c3bbf9ae3
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
```


Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 755D03C639648FB5828D5F1CC9FE9B57 Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128) 42007B01000001A042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBED2442000D020000000400000002000000042000F010000006842005C05000000040000000800000000420093080000000080E9E1875336E415E42007F050000000400000000000000004200700C0100000030420094070000002430613333653833652D356237612D343836352D393634612D3864316333626266396165330000000042006F0100000058420040010000005042004205000000040000000100000000420045010000001842004308000000010755D03C639648FB5828D5F1CC9FE9B57420028050000000400000003000000042002A020000000400000080000000000
3	Client B: Get attribute list In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000004842005C050000000400000000C000000042007901000000304200940700000024306133336538336 52D356237612D343836352D393634612D3864316333626266396165330000000042 Out: uuidKey, attributes={ * } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED24 (Thu Nov 12 12:10:28 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digest Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Initial Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Unique Identifier Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Last Change Date 42007B01000001C842007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBED2442000D020000000400000001000000042000F010000017042005C050000000400000000C0000000042007F0500000004000000000000000042007C0100000148420094070000002430613333653833652D356237612D343836352D393634612D386431633362626639616533000000042000A07000000144372797074 6F67726170686963204C656E6774680000000042000A0700000017437279707 46F6772617068696320416C676F726974686D0042000A0700000005537461746500000042000A0700000006446967657374000042000A070000000C496E697469616C20446174650000000042000A0700000011556E6971756520496465E7469666965720000000000000042000A07000000044E616D650000000042000A0700000018437279707 46F6772617068696320557361676520 4D61736B42000A0700000000B4F626A6563742054797065000000000042000A0700000013436F6E7461637420496E666F726D6174696F6E0000000000042000A07000000104C617374204368616E67652044617465
4	Client B: Get attributes In: uuidKey, attributeNames={‘Name’, ‘ContactInformation’} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information 4200780100000C042007701000000384200690100000020420 06A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000007842005C050000000400000000B0000000042007901000000604200940700000024306133336538336 52D356237612D343836352D393634612D386431633362626639616533000000042000A07000000044E616D650000000042000A0700000013436F6E7461637420496E666F726D6174696F6E0000000000 Out: uuidKey, attributes={ Name={ Name=‘Key1’, NameType=’00000001’ }, ContactInformation=‘Foo’ } Tag: Response Message (0x42007B), Type: Structure (0x01), Data:

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED24 (Thu Nov 12 12:10:28 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Foo 42007B01000001284200 7A01000000484200690100000020420 06A020000000400000001000000004200 6B02000000040000000000000004200 9209000000080000000004AFBED2442000D020000000400000001000000004200 0F01000000D042005C0500000004000000 0B0000000042007F0500000004000000 0000000000042007C01000000A8420094 0700000243061333365383365 2D356237612D343836352D393634612D 3864316333626266396165330000000 4200080100000038420000A07000000 044E616D650000000042000B01000000 2042005507000000044B6579310000000 0420054050000000400000001000000 0042000801000000 3042000A0700000 013436F6E7461637420496E666F726D6174696F6E000000000042000B0700000003466F6F0000000000
5	Client B: Add attribute [batch] In: uuidKey, attribute={ x-attribute1='Value1'} In: uuidKey, attribute={ x-attribute2='Value2' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7A92DDA525EB158A Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value1 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

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


420078010000016042007701000000384200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000042000D020000000400000002000000042000F010000008842005C050000000400000000D0000000042009308000000087A92DDA525EB158A42007901000000604200940700000024306133336538336 52D356237612D343836352D393634612D386431633362626639616533000000004200080100000028420 00A070000000C782D6174747269627574653100000000420 00B070000000656616C7565320000 0
```

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

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

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED25 (Thu Nov 12
12:10:29 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7A92DDA525EB158A
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-
8d1c3bbf9ae3
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value1
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7230F6E4D3BEA249
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-
8d1c3bbf9ae3
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value2


42007B010000019042007A01000000484200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000042009209000000008000000004AFBED2542000D020000000400000002000000004200 0F010000009842005C050000000400000000D0000000042009308000000087A92DDA525EB158A42007F050000000400000000000000000420
```


Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	07C0100000060420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961 65330000000042000801000000C782D6174747269627574653100000000042000B070000000656616 C756531000042000F01000000842005C05000000040000000D0000000042009308000000087230F6E4D3BEA24942007F 05000000040000000000000000042007C0100000060420094070000002430613333653833652D356237612D343836352D3 93634612D38643163336262663961653300000000420008010000002842000A070000000C782D617474726962756532 0000000042000B070000000656616C7565320000
6	Client B: Modify attribute [batch] In: uuidKey, attribute={ x-attribute1='ModifiedValue1' } In: uuidKey, attribute={ x-attribute2='ModifiedValue2' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BA3EA60548ECB699 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a- 8d1c3bbf9ae3 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 321984E716274A3D Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a- 8d1c3bbf9ae3 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2 42007801000001704200770100000038420069010000002042006A020000000400000001000000042006B02000000040 00000000000000042000D020000000400000002000000042000F01000000942005C05000000040000000E0000000042 00930800000008BA3EA60548ECB6994200790100000068420094070000002430613333653833652D356237612D3438363 52D393634612D38643163336262663961653300000000420008010000003042000A070000000C782D6174747269627574 65310000000042000B070000000E4D6F64696669656456616C756531000042000F01000000942005C050000000400000 00E000000004200930800000008321984E716274A3D420079010000006842009407000000243061333365383365 2D3562 37612D343836352D393634612D38643163336262663961653300000000420008010000003042000A070000000C782D617 4747269627574653200000000042000B070000000E4D6F64696669656456616C7565320000 Out: uuidKey, attribute={ x-ttribute1='ModifiedValue1' } Out: uuidKey, attribute={ x-attribute2='ModifiedValue2' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED26 (Thu Nov 12 12:10:30 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BA3EA60548ECB699 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 321984E716274A3D Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2 42007B01000001A042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBED2642000D020000000400000002000000042000F01000000A042005C050000000400000000E000000004200930800000008BA3EA60548ECB69942007F050000000400000000000000000042007C0100000068420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961653300000000420008010000003042000A070000000C782D6174747269627574653100000000042000B070000000E4D6F64696669656456616C7565310000042000F01000000A042005C050000000400000000E000000004200930800000008321984E716274A3D42007F050000000400000000000000000042007C0100000068420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961653300000000420008010000003042000A070000000C782D6174747269627574653200000000042000B070000000E4D6F64696669656456616C7565320000
7	Client B: Delete attribute [batch] In: uuidKey, attributeNames={'x-attribute1'} In: uuidKey, attributeNames={'x-attribute2'} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D5C6DF842DAEECD8 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

```
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 572D4F0D433DAB10
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-
8d1c3bbf9ae3
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2


420078010000013042007701000000384200690100000020420 06A020000000400000001000000004200 6B02000000040
0000000000000004200 0D020000000400000002000000004200 0F01000000704200 5C050000000400000 0F000000042
00930800000008D5C6DF842DAEECD842007901000000484200940700000024306133336538338 52D356237612D3438363
52D393634612D3864316333626266396165330000000042000A070000000C782D617474726962757465310000000042000
0F010000007042005C050000000400000000F000000004200930800000008572D4F0D433DAB1042007901000000484200 9
4070000002430613333653833652D356237612D343836352D393634612D3864316333626266396165330000000042000A
070000000C782D617474726962757465320000000 0
```

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

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

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED26 (Thu Nov 12
12:10:30 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D5C6DF842DAEECD8
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-
8d1c3bbf9ae3
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 572D4F0D433DAB10
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-
8d1c3bbf9ae3
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2


42007B01000001A042007A0100000048420069010000002042006A020000000400000001000000004200 6B02000000040
0000000000000004200920900000008000000004AFBED2642000D020000000400000002000000004200 0F01000000A042
005C050000000400000000F000000004200930800000008D5C6DF842DAEECD842007F050000000400000000000000004200
07C010000006842009407000000243061333365383365 2D356237612D343836352D393634612D3864316333626266396 1
```


Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	653300000000420008010000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F6 4696669656456616C756531000042000F01000000A042005C0500000004000000F000000004200930800000008572D4F 0D433DAB1042007F0500000004000000000000000042007C0100000068420094070000024306133336538336352D35623 7612D343836352D393634612D3864316333626266396165330000000042000801000000303042000A070000000C782D6174 74726962757465320000000042000B070000000E4D6F64696669656456616C7565320000
8	Client A: Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 420078010000009042007701000000384200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000000042000D020000000400000001000000004200 0F01000000484200 5C050000000400000014000000004200 7F050000000400000000000000000042007C0100000030420094070000002430613333653833652D356237612D343836352D393634612D3864316333626266396165330000000042000801000000303042000A070000000C782D6174747269627574653200000000420 0B070000000E4D6F6469666965645661 6C7565320000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED27 (Thu Nov 12 12:10:31 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B020000000400000000000000000042009209000000008000000004AFBED2742000D020000000400000001000000004200 0F010000005842005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002430613333653833652D356237612D343836352D393634612D3864316333626266396165330000000042000801000000303042000A070000000C782D6174747269627574653200000000420 0B070000000E4D6F6469666965645661 6C7565320000
9	Client A: Get (symmetric key) In: uuidKey

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
	
	42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000004842005C050000000400000000A00000000420079010000003042009407000000243061333365383365 2D356237612D343836352D393634612D386431633362626639616533000000000
	
	Out: Operation Failed, Item Not Found
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED27 (Thu Nov 12 12:10:31 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Failed)
	  Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x00000001 (Item Not Found)
	  Tag: Result Message (0x42007D), Type: Text String (0x07), Data: No Cryptographic Object found with given Unique Identifier
	
	42007B01000000D042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBED2742000D020000000400000001000000042000F010000007842005C050000000400000000A0000000042007F050000000400000001000000042007E050000000400000001000000042007D070000003A4E6F2043727970746F6772617068696320 4F626A65637420666F756E642077697468206769766 56E2055 6E697175652049646 56E74696669657200000000000000

10	Client A:
	Destroy (template)
	In: uuidTemplate
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 45d8629a-9ad1-41b3-9d09-941f2a595da3 420078010000009042007701000000384200690100000020420 06A0200000040000000100000000420 06B020000000400000000000000042000D020000000400000001000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002434356438363239612D396164312D343162332D396430392D3934316632613539356 4613300000000 Out: uuidTemplate Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED27 (Thu Nov 12 12:10:31 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 45d8629a-9ad1-41b3-9d09-941f2a595da3 42007B01000000B042007A0100000048420069010000002042006A0200000040000000100000000420 06B020000000400000000000000042009209000000080000000004AFBED2742000D020000000400000001000000004200F010000005842 005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002434356438363239612D396164312D343162332D396430392D3934316632613539356 4613300000000
11	Client A: Get (template) In: uuidTemplate Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 45d8629a-9ad1-41b3-9d09-941f2a595da3 420078010000009042007701000000384200690100000020420 06A0200000040000000100000000420 06B020000000400000000000000042000D020000000400000001000000042000F010000004842005C050000000400000000A0000000042 00790100000030420094070000002434356438363239612D396164312D343162332D396430392D3934316632613539356

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	4613300000000 Out: Operation Failed, Item Not Found Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED27 (Thu Nov 12 12:10:31 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Failed) Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x00000001 (Item Not Found) Tag: Result Message (0x42007D), Type: Text String (0x07), Data: No Cryptographic Object found with given Unique Identifier 42007B01000000D042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBED2742000D020000000400000001000000042000F010000007842005C050000000400000000A0000000042007F050000000400000001000000042007E050000000400000001000000042007D070000003A4E6F2043727970746F6772617068696320 4F626A65637420666F756E642077697468206769766 56E2055 6E697175652049646 56E74696669657200000000000

3.2 Use-case: Asynchronous Locate

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

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

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

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1


42007801000001904200770100000038420069010000002042006A020000000400000001000000042006B02000000040
00000000000000042000D020000000400000001000000042000F010000014842005C050000000400000001000000042
00790100000130420057050000000400000002000000004200910100000118420008010000003042000A0700000017437
27970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200
0A0700000014437279707 46F67726170686963204C656E6774680000000042000B020000000400000080000000042000
80100000038420 00A07000000044E616D650000000042000B0100000020420055070000000 44B65793100000000420054
0500000004000000010000000042000801000000 3042000A0700000018437279707 46F6772617068696320557361676 52
04D61736B42000B020000000400000004000000004200080100000028420 00A070000000C4F626A6563742047726F7570
0000000042000B070000000647726F7570310000
```

Out: objectType = ‘00000002’, uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED28 (Thu Nov 12
12:10:32 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
```


Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBED2842000D020000000400000001000000042000F010000006842005C050000000400000001000000042007F050000000400000000000000042007C0100000040420057050000000400000002000000042009407000000243935613065366233 2D386564632D346666622D613838652D653136343533396462636100000000
1	Client B: Locate (symmetric key by name) In: asynchronousIndicator='TRUE', attributes={ objectType = '00000002', Name={ Name='Key1', NameType='00000001'} } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 4200780100000E042007701000000484200690100000020420 06A020000000400000001000000042006B02000000040000000000000042000700600000008000000000000000142000D020000000400000001000000042000F010000008842005C050000000400000008000000004200790100000070420008010000002842000A070000000B4F626A6563742054797065000000000042000B050000000400000002000000042000801000000384 2000A07000000044E616D650000000042000B010000002042005507000000044B65793100000000420054050000000400000001000000000 Out: asyncCorrValue1 Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED28 (Thu Nov 12 12:10:32 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Pending) Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 130BC369AF005A7F 42007B01000000842007A01000000484200690100000020420 06A020000000400000001000000004200 6B02000000040000000000000000042009209000000080000000 04AFBED2842000D020000000400000001000000004200 0F010000003042005C05000000040000000800000000420 07F05000000040000000200000000420006080000000 8130BC369AF005A7F
2	Client B: Poll* In: asyncCorrValue1 Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 130BC369AF005A7F 42007801000000704200770100000038420069010000002042006A020000000400000001000000004200 6B02000000040000000000000000042000D020000000400000001000000004200 0F010000002842005C05000000040000001A00000000420079010000001042000608000000008130BC369AF005A7F Out: uuidKey1 Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED28 (Thu Nov 12 12:10:32 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca 42007B01000000B042007A01000000484200690100000020420 06A020000000400000001000000004200 6B02000000040

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	00000000000000042009209000000080000000004AFBED2842000D020000000400000001000000004200F010000005842005C050000000400000008000000042007F050000000400000000000000042007C0100000030420094070000002439356130653662332D386564632D346666622D613838652D65313634353339646263636100000000
3	Client B: Get (symmetric key) In: uuidKey1 Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca 42007801000000904200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000042000D020000000400000001000000004200F010000004842005C050000000400000000A000000004200790100000030420094070000002439356130653662332D386564632D346666622D613838652D65313634353339646263636100000000 Out: objectType = ‘00000002’, uuidKey1, symmetricKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: BEF01F82DFB4682A01C2A08413834AAB Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	42007B01000001204200 7A0100000048420069010000002042006A020000000400000001000000004200 6B02000000040000000000000042009209000000008000000004AFBED2942000D020000000400000001000000004200 0F01000000C842005C05000000040000000A0000000042007F050000000400000000000000000042007C01000000A042005705000000040000000200000004200940700000024393561306536623 32D386564632D346666622D613838652D653136343533396462636361000000042008F0100000058420040010000005042004205000000040000000100000000420045010000001842004308000000010BEF01F82DFB4682A01C2A08413834AAB4200280500000004000000030000000042002A0200000004000000008000000000
4	Client B: Locate (symmetric key by group) In: asynchronousIndicator='TRUE', attributes={ objectType = '00000002', ObjectGroup='Group1' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1 4200780100000D042007701000000484200690100000020420 06A020000000400000001000000004200 6B02000000040000000000000042007060000000800000000000000014200 0D020000000400000001000000004200 0F010000007842005C05000000040000000800000000420079010000006042000801000000284200 0A070000000B4F626A6563742054797065000000000042000B05000000040000000200000004200080100000028420 00A070000000C4F626A6563742047726F757000000000042000B070000000647726F7570310000 Out: asyncCorrValue2 Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Pending) Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 48D43C207CD1FB3A 42007B01000000884200 7A0100000048420069010000002042006A020000000400000001000000004200 6B02000000040

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	00000000000000042009209000000008000000004AFBED2942000D020000000400000001000000042000F010000003042 005C050000000400000008000000042007F050000000400000002000000042000608000000848D43C207CD1FB3A
5	Client B: Poll* In: asyncCorrValue2 Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 48D43C207CD1FB3A 42007801000000704200770100000038420069010000002042006A020000000400000001000000042006B02000000040 00000000000000042000D020000000400000001000000042000F010000002842005C050000000400000001A0000000042 00790100000010420006080000000848D43C207CD1FB3A Out: uuidKey2 Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e- e164539dbcca 42007B01000000B042007A01000000484200690100000020420 06A020000000400000001000000042006B02000000040 00000000000000042009209000000008000000004AFBED2942000D020000000400000001000000042000F010000005842 005C050000000400000008000000042007F050000000400000000000000042007C0100000030420094070000002439 3 56130653662332D386564632D346666622D613838652D65313634353339646263636100000000
6	Client B: Get (symmetric key) In: uuidKey2 Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data:

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B02000000040000000000042000D020000000400000001000000042000F010000004842005C050000000400000000A0000000420079010000003042009407000000243935613065366233 2D386564632D346666622D613838652D6531363435333964626 3636100000000 Out: objectType = ‘00000002’, uuidKey2, symmetricKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: BEF01F82DFB4682A01C2A08413834AAB Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128) 42007B010000012042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000042009209000000080000000004AFBED2942000D020000000400000001000000042000F01000000C842005C050000000400000000A0000000042007F050000000400000000000000000042007C01000000A04200570500000004000000020000000042009407000000243935613065366233 2D386564632D346666622D613838652D6531363435339646263636100000000042008F010000005842004001000000504200420500000004000000010000000042004501000000184200430800000010BEF01F82DFB4682A01C2A08413834AAB42002805000000040000000300000000042002A020000000400000008000000000
7	Client B: Locate (symmetric key by name) In: asynchronousIndicator=’TRUE’, attributes={ objectType = ‘00000002’, Name= { Name=‘Key1’,

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	NameType=’00000001’ } }
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
	  Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
	  Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
	  Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
	  Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
	
	42007801000000E042007701000000484200690100000020420 06A020000000400000001000000004200 6B02000000040 0000000000000004200070600000008000000000000000142000D020000000400000001000000004200 0F010000008842 005C050000000400000008000000004200790100000070420008010000002842000A070000000B4F626A6563742054797 065000000000042000B050000000400000002000000004200080100000038420 00A070000000044E616D65000000004200 0B010000002042005507000000044B65793100000000420054050000000400000001000000000
	
	Out: asyncCorrValue5
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Pending)
	  Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 4D6BBFC35FE57FBA
	
	42007B010000008842007A010000004842006901000002042006A020000000400000001000000004200 6B02000000040 0000000000000004200920900000008000000004AFBED2942000D020000000400000001000000004200 0F010000003042 005C050000000400000008000000004200 7F050000000400000002000000004200060800000008 4D6BBFC35FE57FBA

8	Client B: Cancel

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	In: asyncCorrValue5
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000019 (Cancel)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 4D6BBFC35FE57FBA
	
	42007801000000704200770100000038420069010000002042006A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000002842005C05000000040000001900000000420078010000007042007701000000384200690100000020420069010000002042006A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000002842005C05000000040000001900000000420079010000001042000608000000084D6BBFC35FE57FBA
	
	Out: asyncCorrValue5, CancelResult=’00000001’
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED29 (Thu Nov 12 12:10:33 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000019 (Cancel)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 4D6BBFC35FE57FBA
	  Tag: Cancellation Result (0x420012), Type: Enumeration (0x05), Data: 0x00000001 (Cancelled)
	
	42007B01000000A042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBED2942000D020000000400000001000000042000F010000004842005C05000000040000001900000000420078010000007042007701000000384200690100000020420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBED2942000D020000000400000001000000042000F010000004842005C05000000040000001900000000420079F05000000040000000000000000042007C010000002042000608000000084D6BBFC35FE57FBA420012050000000400000010000000

9	Client A:
	Destroy (symmetric key)
	In: uuidKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000004842005C050000000400000014000000042007901000000304200940700000024393561306536623 32D386564632D346666622D613838652D6531363435333964626 3636100000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2A (Thu Nov 12 12:10:34 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-e164539dbcca 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBED2A42000D020000000400000001000000042000F010000005842005C050000000400000014000000042007F050000000040000000000000000042007C0100000030420094070000002439356130653662332D386564632D346666622D613838652D653136343533396462636361000000000

* = executed until response is ready

4 Key life cycle support

4.1 Use-case: Revoke scenario

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

Time	Client A

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

0	Client A: Create (symmetric key) In: objectType = ‘00000002’, attributes={ CryptographicAlgorithm=’AES’, CryptographicLength=’128’, Name={ NameValue=‘Key1’, NameType=’00000001’ }, CryptographicUsageMask=‘00000004’ } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt) 42007801000001604200770100000038420069010000002042006A020000000400000001000000042006B02000000040 00000000000000042000D020000000400000001000000042000F01000001184200 5C05000000040000000100000000042 00790100000100420057050000000400000002000000004200910100000 0E84200080100000030420 00A0700000017437 27970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042 00 0A0700000014437279707 46F6772617068696320 4C656E6774680000000042000B020000000400000080000000004200 0 801000000384200 0A07000000044E616D650000000042000B0100000020420055070000000 44B6579310000000042005 4 05000000040000000100000000420008010000003042000A0700000018437279707 46F6772617068696320 55736167652 04D61736B42000B020000000400000004000000 0 Out: objectType = ‘00000002’, uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 42007B01000000C042007A01000000484200690100000020420 06A020000000400000001000000004200 6B02000000040 0000000000000004200920900000008000000004AFBED2B42000D020000000400000001000000004200 0F010000006842 005C050000000400000001000000004200 7F050000000400000000000000004200 7C010000004042005705000000040000 0000200000000420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164 613900000000
1	Client A: Get attribute In: uuidKey, attributeName={‘State’} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 4200780100000 0A042007701000000384200690100000020420 06A020000000400000001000000004200 6B02000000040 0000000000000004200 0D020000000400000001000000004200 0F0100000058420 05C050000000400000000B0000000042 0079010000004042009407000000243231643238623 8612D303664662D343363302D623732662D326131363133633361646139000000000420 00A0700000005537461746500000 0 Out: uuidKey, attribute={ State=‘00000001’ } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000001 (Pre-Active) 42007B01000000D842007A0100000048420069010000002042006A020000000400000001000000042006B02000000040 000000000000004200920900000008000000004AFBED2B42000D020000000400000001000000042000F010000008042 005C05000000040000000B0000000042007F05000000040000000000000042007C0100000058420094070000002432 3 16432386238612D303664662D343363302D623732662D3261313631363333616461390000000042000801000000204200 0A0700000005537461746500000042000B05000000040000000100000000
2	Client A: Add attribute In: uuidKey, attribute={ ActivationDate='2' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f- 2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000000000002 (Thu Jan 01 01:00:02 CET 1970) 42007801000000C042007701000000384200690100000020 42006A020000000400000001000000042006B02000000040 000000000000000042000D020000000400000001000000042000F010000007842005C05000000040000000D0000000042 00790100000060420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616 461390000000042000801000000 2842000A070000000F41637469766174696F6E204617465004 2000B09000000080000 000000000002 Out: uuidKey, attribute={ ActivationDate='2' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000000000002 (Thu Jan 01 01:00:02 CET 1970) 42007B01000000E042007A0100000048420069010000002042006A020000000400000001000000042006B02000000400000000000004200920900000008000000004AFBED2B42000D020000000400000001000000042000F010000008842005C050000000400000000D0000000042007F050000000400000000000000042007C0100000060420094070000002432316432386238612D303664662D343363302D623732662D326131363136333361646139000000004200801000000284200A070000000F41637469766174696F6E20446174650042000B0900000008000000000000002
3	Client A: Get attribute In: uuidKey, attributeName={ ‘State’ } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 4200780100000A042007701000000384200690100000020420 06A020000000400000001000000042006B02000000400000000000004200D020000000400000001000000042000F010000005842005C050000000400000000B000000004200790100000040420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000420080100000028420 00A070000000F41637469766174696F6E20446174650042000B0900000008000000000000002 Out: uuidKey, attribute={ State=‘00000002’ } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active) 42007B01000000D842007A0100000048420069010000002042006A020000000400000001000000042006B02000000040 00000000000000042009209000000080000000004AFBED2B42000D020000000400000001000000042000F010000008042 005C0500000004000000B0000000042007F0500000004000000000000000042007C0100000058420094070000002432 3 16432386238612D303664662D343363302D623732662D326131363136333361646139000000004200080100000020420 0 0A0700000005537461746500000042000B0500000004000000200000000
4	Client B: Locate (symmetric key by name) In: objectType = ‘00000002’, attributes={ Name={ Name=‘Key1’, NameType=’00000001’ } } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 4200780100000D042007701000000384200690100000020420 06A020000000400000001000000042006B02000000040 00000000000000042000D020000000400000001000000042000F010000008842005C0500000004000000080000000042 00790100000070420008010000002842000A070000000B4F626A6563742054797065000000000042000B0500000004000 0000200000000420008010000003842000A07000000044E616D650000000042000B0100000020420055070000000044B65 7931000000004200540500000004000000100000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBED2B42000D020000000400000001000000042000F010000005842005C05000000040000000800000004200 7F05000000040000000000000004200 7C0100000030420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000
5	Client B: Get (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 4200780100000090420077010000003842006901000000204200 6A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000004842005C05000000040000000A0000000042007901000000304200940700000024323164323862386 12D303664662D343363302D623732662D32613136313633336164613900000000 Out: objectType = ‘00000002’, uuidKey, symmetricKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: EF7833AB15F5A1EE5874BC0D9BBC4BE7

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128) 42007B01000012042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040 00000000000000042009209000000080000000004AFBED2B42000D020000000400000001000000042000F01000000C842 005C0500000004000000A0000000042007F0500000004000000000000000042007C01000000A0420057050000000400 0000200000000420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164 6139000000042008F0100000058420040010000005042004205000000040000000100000004200450100000018420043 08000000010EF7833AB15F5A1EE5874BC0D9BBC4BE74200280500000004000000030000000042002A0200000004000000 8000000000
6	Client B: Revoke (symmetric key as compromised) In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceTime='6' Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data: Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000002 (Key Compromise) Tag: Compromise Occurrence Date (0x420021), Type: Date-Time (0x09), Data: 0x0000000000000006 (Thu Jan 01 01:00:06 CET 1970) 42007801000000B84200770100000038420069010000002042006A020000000400000001000000042006B02000000040 00000000000000042000D020000000400000001000000042000F010000007042005C050000000400000013000000004200 7901000000584200940700000024323164323862386238612D303664662D343363302D623732662D326131363133633336164 613900000000420081010000001042008205000000040000000200000004200210900000008000000000000006 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12 12:10:35 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	2a161633ada9 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040 0000000000000042009209000000080000000004AFBED2B42000D020000000400000001000000042000F010000005842 005C0500000004000000130000000042007F0500000004000000000000000042007C0100000030420094070000002432 3 16432386238612D303664662D343363302D623732662D32613136313633336164613900000000
7	Client B: Get attribute In: uuidKey, attributeName={ 'State' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f- 2a161633ada9 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 4200780100000A042007701000000384200690100000020420 06A020000000400000001000000042006B02000000040 0000000000000042000D020000000400000001000000042000F010000005842005C0500000004000000B0000000042 00790100000040420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164 6139000000042000A0700000005537461746500000 0 Out: uuidKey, attribute={ State='00000004' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2C (Thu Nov 12 12:10:36 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f- 2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Compromised) 42007B01000000D842007A0100000048420069010000002042006A020000000400000001000000042006B02000000040 0000000000000042009209000000080000000004AFBED2C42000D020000000400000001000000042000F010000008042 005C0500000004000000B0000000042007F0500000004000000000000000042007C0100000058420094070000002432 3

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	16432386238612D303664662D343363302D623732662D3261313631363333616461390000000042000801000000204200A0700000005537461746500000042000B0500000004000000040000000
8	Client A: Get attribute list In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 42007801000000904200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400000000100000000420 0D020000000400000001000000004200 0F010000004842005C050000000400000000C0000000420079010000003042009407000000243231643238623 8612D303664662D343363302D623732662D32613136313633336164613900000000 Out: uuidKey, attributes = { * } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2C (Thu Nov 12 12:10:36 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Compromise Occurrence Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Compromise Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digest Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Initial Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Revocation Reason Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Unique Identifier Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Last Change Date 42007B010000022042007A01000000484200690100000020420 06A020000000400000001000000004200 6B02000000040 00000000000000042009209000000008000000004AFBED2C42000D020000000400000001000000004200 0F01000001C842 005C050000000400000000C0000000042007F050000000400000000000000000042007C01000001A0420094070000002432 3 16432386238612D303664662D343363302D623732662D32613136313633336164613900000000042000A07000000144372 7970746F67726170686963204C656E6774680000000042000A0700000017437279707 46F6772617068696320416C676F7 26974686D0042000A0700000005537461746500000042000A070000001A436F6D70726F6D697365204F6363757272656E 6365204461746500000000000042000A070000000F436F6D70726F6D6973652044617465004 2000A07000000064469676 57374000042000A070000000C496E697469616C20446174650000000042000A070000000F41637469766174696F6E2044 6174650042000A0700000011526576 6F636174696F6E20526561736F6E000000000000042000A07000000011556E69717 565204964656E74696669657200000000000000042000A07000000044E616D650000000042000A0700000018437279707 4 6F67726170686963205573616765204D61736B42000A070000000B4F626A6563742054797065000000000042000A07000 000104C617374204368616E67652044617465
9	Client A: Get attributes In: uuidKey, attributeName = { ‘State’ } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 42007801000000A042007701000000384200690100000020420 06A020000000400000001000000004200 6B02000000040 00000000000000042000D020000000400000001000000004200 0F01000005842005C050000000400000000B0000000042 00790100000040420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000042000A07000000055374617465000000 Out: uuidKey, attribute={ State=‘00000004’ } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2C (Thu Nov 12 12:10:36 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Compromised) 42007B01000000D842007A0100000048420069010000002042006A020000000400000001000000042006B02000000040 00000000000000042009209000000080000000004AFBED2C42000D020000000400000001000000042000F010000008042 005C0500000004000000B0000000042007F0500000004000000000000000042007C0100000058420094070000002432 3 16432386238612D303664662D343363302D623732662D326131363136333361646139000000004200080100000020420 0 0A0700000005537461746500000042000B0500000004000000040000000
10	Client A: Add attribute [batch] In: uuidKey, attribute={ x-attribute1='Value1' } In: uuidKey, attribute={ x-attribute2='Value2' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 9D407FFB45C95672 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f- 2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value1 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: D62107C3158409D8 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f- 2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value2 42007801000001604200770100000038420069010000002042006A020000000400000001000000042006B02000000040 00000000000000042000D020000000400000002000000042000F0100000008842005C0500000004000000D0000000042 009308000000089D407FFB45C9567242007901000000604200940700000024323164323862386 12D303664662D3433633 02D623732662D326131363136333361646139000000004200080100000028420 00A070000000C782D6174747269627574 653100000000042000B0700000006566 16C756531000042000F0100000088420 05C0500000004000000D0000000042009 30800000008D62107C3158409D842007901000000604200940700000024323164323862386 12D303664662D343363302D 623732662D326131363136333361646139000000004200080100000028420 00A070000000C782D6174747269627574653 20000000042000B0700000006566 16C7565320000 Out: uuidKey, attribute={ x-attribute1='Value1' } Out: uuidKey, attribute={ x-attribute2='Value2' }

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

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


42007B010000019042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040
000000000000000420092090000000800000000 4AFBED2C42000D020000000400000002000000042000F010000009842
005C0500000004000000D000000004200930800000089D407FFB45C9567242007F0500000004000000000000000420
07C0100000060420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164
6139000000004200080100000028420 00A070000000C782D617474726962757465310000000042000B070000000656616
C756531000042000F010000009842005C0500000004000000D000000004200930800000008D62107C3158409D842007F
0500000004000000000000000042007C0100000060420094070000002432316432386238612D303664662D343363302D6
23732662D32613136313633336164613900000000420008010000002842000A070000000C782D61747472696275746532
0000000042000B070000000656616C7565320000
```

11

Client A:

Modify attribute [batch]

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

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

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
```


Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

```
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 47FB42CCECA3F6EC
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-
2a161633ada9
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 08019A230A05E9E1
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-
2a161633ada9
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2


420078010000017042007701000000384200690100000020420 06A020000000400000001000000042006B02000000040
000000000000000042000D020000000400000002000000042000F010000009042005C050000000400000000E0000000042
009308000000847FB42CCECA3F6EC4200790100000068420094070000002432316432386238612D303664662D3433633
02D623732662D326131363136333361646139000000004200080100000030420 00A070000000C782D6174747269627574
653100000000042000B070000000E4D6F64696669656456616C756531000042000F010000009042005C050000000400000
00E000000004200930800000000808019A230A05E9E1420079010000006842009407000000243231643238623 8612D3036
64662D343363302D623732662D326131363136333361646139000000004200080100000030420 00A070000000C782D617
4747269627574653200000000042000B070000000E4D6F64696669656456616C7565320000


Out: uuidKey, attribute={ x-attribute1='ModifiedValue1' }
Out: uuidKey, attribute={ x-attribute2='ModifiedValue2' }


Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2D (Thu Nov 12
12:10:37 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 47FB42CCECA3F6EC
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-
2a161633ada9
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 08019A230A05E9E1
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
```


Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2 42007B01000001A042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040 00000000000000042009209000000080000000004AFBED2D42000D020000000400000002000000042000F01000000A042 005C0500000004000000E000000004200930800000000847FB42CCECA3F6EC42007F0500000004000000000000000420 07C0100000068420094070000002432316432386238612D303664662D343363302D623732662D3261313631336336164 6139000000004200080100000030420 00A070000000C782D617474726962757465310000000042000B070000000E4D6F6 4696669656456616C756531000042000F01000000A042005C0500000004000000E000000042009308000000808019A 230A05E9E142007F0500000004000000000000000042007C0100000068420094070000002432316432386238612D30366 4662D343363302D623732662D32613136313633336164613900000000420008010000003042000A070000000C782D6174 74726962757465320000000042000B070000000E4D6F64696669656456616C7565320000
12	Client A: Delete attribute [batch] In: uuidKey, attributeNames={ ‘x-attribute1’ } In: uuidKey, attributeNames={ ‘x-attribute2’ } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3E2C080FA8806057 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1 Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 9D55988D43D23B82 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 42007801000001304200770100000038420069010000002042006A020000000400000001000000042006B02000000040 00000000000000042000D020000000400000002000000042000F010000007042005C0500000004000000F0000000042 009308000000083E2C080FA880605742007901000000484200940700000024323164323862386 12D303664662D3433633 02D623732662D32613136313633336164613900000000420 00A070000000C782D617474726962757465310000000042000 0F010000007042005C0500000004000000F000000004200930800000089D55988D43D23B824200790100000048420 09 407000000243231643238623 8612D303664662D343363302D623732662D32613136313633336164613900000000420 00A 070000000C782D617474726962757465320000000 0 Out: uuidKey, attributeNames={ ‘x-attribute1’ } Out: uuidKey, attributeNames={ ‘x-attribute2’ }

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2D (Thu Nov 12 12:10:37 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
	  Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3E2C080FA8806057
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
	  Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
	  Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 9D55988D43D23B82
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9
	  Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	  Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
	  Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2
	
	42007B01000001A042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040
	00000000000000042009209000000080000000004AFBED2D42000D020000000400000002000000042000F01000000A042
	005C050000000400000000F000000004200930800000083E2C080FA880605742007F0500000004000000000000000420
	07C0100000068420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164
	6139000000004200080100000030420000A070000000C782D617474726962757465310000000042000B070000000E4D6F6
	4696669656456616C756531000042000F01000000A042005C050000000400000000F000000004200930800000089D5598
	8D43D23B8242007F0500000004000000000000000042007C0100000068420094070000002432316432386238612D30366
	4662D343363302D623732662D32613136313633336164613900000000420008010000003042000A070000000C782D6174
	74726962757465320000000042000B070000000E4D6F64696669656456616C7565320000

13	Client A:
	Get (symmetric key)
	In: uuidKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000004842005C050000000400000000A000000004200790100000030420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000
	Out: objectType = ‘00000002’, uuidKey, symmetricKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2D (Thu Nov 12 12:10:37 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: EF7833AB15F5A1EE5874BC0D9BBC4BE7 Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128) 42007B010000012042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBED2D42000D020000000400000001000000042000F01000000C842005C050000000400000000A0000000042007F050000000400000000000000042007C01000000A042005705000000040000000000000042009407000000243231643238623861 2D303664662D343363302D623732662D326131363133633361646139000000042008F0100000058420040010000005042004205000000040000000100000000420045010000001842004308000000010EF7833AB15F5A1EE5874BC0D9BBC4BE74200280500000004000000030000000042002A020000000400000080000000
14	Client A: Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000004842005C050000000400000014000000042007901000000304200940700000024323164323862386238612D303664662D343363302D623732662D32613136313631363336164613900000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2E (Thu Nov 12 12:10:38 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000008000000004AFBED2E42000D020000000400000001000000042000F010000005842005C050000000400000014000000042007F050000000400000000000000042007C0100000030420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000

5 Auditing and reporting

5.1 Use-case: Get usage allocation scenario

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

Time	Client A
0	Client A:

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

Create (symmetric key)

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

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt)
```

```
42007801000001604200770100000038420069010000002042006A020000000400000001000000004200 6B020000000400
0000000000000042000D020000000400000001000000004200 0F0100000118420050C0500000004000000010000000042000
790100000100420057050000000400000002000000004200 9101000000E84200080100000030420 00A0700000017437279
70746F67726170686963204 16C676F726974686D0042000B0500000004000000030000000042000801000000304 2000A07
0000001443727970746F67726170686963204C656E6774680000000042000B020000000400000080000000004200080100
00003842000A07000000044E616D650000000042000B0100000020420055070000000044B65793100000000420054050000
0004000000010000000042000801000000304 2000A0700000018437279707 46F6772617068696320557361676520 4D6173
6B42000B020000000400000040000000 0
```

Out: objectType = ‘00000002’, uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2E (Thu Nov 12
12:10:38 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
```


Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f 42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042009209000000080000000004AFBED2E42000D020000000400000001000000042000F010000006842005C050000000400000001000000042007F050000000400000000000000042007C0100000040420057050000000400000020000000042009407000000243664326235353638 2D643862342D343064312D393930642D346261306264346666373666 00000000
1	Client A: Add attribute [batch] In: uuidKey, attribute={ ActivationDate='2' } In: uuidKey, attribute={ ProtectStopDate='<*NOW+10min*>' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 33150E6CB1ACF869 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000000000002 (Thu Jan 01 01:00:02 CET 1970) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: CF90BC88AE42CBC2 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004AFBEF86 (Thu Nov 12 12:20:38 CET 2009) 42007801000001684200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042000D020000000400000002000000042000F010000008842005C050000000400000000D000000004200930800000000833150E6CB1ACF8694200790100000060420094070000002436643262353536382D643862342D343064312D393930642D346261306264346666373666000000000420008010000003042000A070000001150726F746563742053746F7020446174650000000000000042000B090000000800000000 4AFBEF86

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Out: uuidKey, attribute={ ActivationDate='2' } Out: uuidKey, attribute={ ProtectStopDate='<*NOW+10min*>' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2E (Thu Nov 12 12:10:38 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 33150E6CB1ACF869 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000000000002 (Thu Jan 01 01:00:02 CET 1970) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: CF90BC88AE42CBC2 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004AFBEF86 (Thu Nov 12 12:20:38 CET 2009) 42007B01000001984200 7A01000000484200690100000020420 06A020000000400000001000000004200 6B020000000400000000000042009209000000080000000004AFBED2E42000D020000000400000002000000004200 0F01000000984200 5C05000000040000000D000000004200930800000000833150E6CB1ACF86942007F05000000040000000000000000042007C 0100000060420094070000002436643262353536382D643862342D343064312D393930642D34626130626434666663736660 0000000042000801000000284200 0A070000000F41637469766174696F6E204617465004200 0B09000000080000000000000000242000F01000000A042005C05000000040000000D000000004200930800000008CF90BC88AE42CBC242007F050000 0004000000000000000000042007C0100000068420094070000002436643262353536382D643862342D343064312D393930642D34626130626434666637366600000000420008010000003042000A07000000115072 6F746563742053746F7020446174650000000000000000042000B09000000008000000004AFBEF86
2	Client A: Add Attribute In: uuidKey, attribute={ UsageLimits={ UsageLimitsTotalBytes='1000'} } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Usage Limits Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Usage Limits Total Bytes (0x420098), Type: Big Integer (0x04), Data: 03E8 (1000) 42007801000000C84200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042000D020000000400000001000000042000F010000008042005C050000000400000000D000000004200790100000068420094070000002436643262353536382D643862342D343064312D393930642D34626130626434666637366600000004200080100000030420004A070000000C5573616765204C696D6974730000000042000B010000001042009804000000800000000000003E8 Out: uuidKey, attribute={ UsageLimits={ UsageLimitsTotalBytes= ‘1000’, UsageLimitsByteCount=‘1000’} } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2F (Thu Nov 12 12:10:39 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Usage Limits Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Usage Limits Total Bytes (0x420098), Type: Big Integer (0x04), Data: 00000000000003E8 (1000) Tag: Usage Limits Byte Count (0x420096), Type: Big Integer (0x04), Data: 00000000000003E8 (1000) 42007B01000000F842007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042009209000000080000000004AFBED2F42000D020000000400000001000000042000F01000000A042005C050000000400000000D0000000042007F050000000400000000000000042007C0100000078420094070000002436643262353536382D643862342D343064312D393930642D34626130626434666637366600000000420008010000004042000A070000000C5573616765204C696D6974730000000042000B010000002042009804000000080000000000003E842009604000000800000000000003E8
3	Client B: Locate (symmetric key by name) In: objectType = ‘00000002’, attributes={ Name={ Name=‘Key1’, NameType= ‘00000001’} }

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007801000000D042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000042000D020000000400000001000000042000F01000000884200 5C050000000400000008000000042007900100000070420008010000002842000A070000000B4F626A656374205479706500000000042000B0500000004000000020000000042000801000000384200 0A07000000044E616D650000000042000B01000000204200550700000004 4B65793100000004200540500000004000000010000000042005405000000040000001000000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2F (Thu Nov 12 12:10:39 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f 42007B01000000B042007A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000042009209000000080000000 04AFBED2F42000D020000000400000001000000042000F01000000584200 5C050000000400000008000000042007F050000000400000000000000042007C01000000304200940700000024366432 62353536382D643862342D343064312D393930642D346261306264346666373666000000000
4	Client B: Get (symmetric key) In: uuidKey

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f
	
	42007801000000904200770100000038420069010000002042006A020000000400000001000000042006B020000000400000000000000042000D020000000400000001000000042000F01000000484200 5C05000000040000000A000000042007F050000000400000000000000042007C01000000A042005705000000040000000200000004200940700000024366432623535363 82D643862342D343064312D393930642D34626130626434666637366600000000

	Out: objectType = ‘00000002’, uuidKey, symmetricKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2F (Thu Nov 12 12:10:39 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f
	  Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
	  Tag: Key Block (0x420040), Type: Structure (0x01), Data:
	  Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
	  Tag: Key Value (0x420045), Type: Structure (0x01), Data:
	  Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 7C228050CE4FADBFF51227C891117F9C
	  Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
	  Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
	
	42007B010000012042007A0100000048420069010000002042006A020000000400000001000000042006B020000000400000000000000042009209000000080000000 4AFBED2F42000D020000000400000001000000042000F01000000C842005C05000000040000000A000000042007F050000000400000000000000042007C01000000A042005705000000040000000200000004200940700000024366432623535363 82D643862342D343064312D393930642D34626130626434666637366600000000420 08F010000005842004001000000504200420500000004000000010000000042004501000000184200430800000107C228050CE4FADBFF51227C891117F9C42002805000000040000000300000000420 02A020000000400000080000000

5	Client B:

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Get usage allocation
	In: uuidKey, UsageLimitsByteCount='500'
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)
	  Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f
	  Tag: Usage Limits Byte Count (0x420096), Type: Big Integer (0x04), Data: 01F4 (500)
	
	42007801000000A042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000042000D020000000400000001000000042000F01000000584200790100000040420094070000002436643262353536382D643862342D343064312D393930642D34626130626434666637366000000004200960400000008000000000000001F4
	
	Out: uuidKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	  Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2F (Thu Nov 12 12:10:39 CET 2009)
	  Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	  Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)
	  Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	  Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	  Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f
	
	42007B01000000B042007A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000042009209000000080000000004AFBED2F42000D020000000400000001000000042000F01000000584200 5C050000000400000011000000042007F050000000400000000000000042007C0100000030420094070000002436643262353536382D643862342D343064312D393930642D34626130626434666637366600000000

6	Client A:
	Get usage allocation
	In: uuidKey, UsageLimitsByteCount='500'
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	  Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f Tag: Usage Limits Byte Count (0x420096), Type: Big Integer (0x04), Data: 01F4 (500) 42007801000000A042007701000000384200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000042000D020000000400000001000000004200 0F01000000584200 5C050000000400000011000000004200 790100000040420094070000002436643262353536382D643862342D343064312D393930642D346261306264346666373666000000042009604000000080000000000001F4 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2F (Thu Nov 12 12:10:39 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f 42007B01000000B042007A01000000484200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000042009209000000080000000004AFBED2F42000D020000000400000001000000004200 0F01000000584200 5C050000000400000011000000004200 7F050000000400000000000000000042007C0100000030420094070000002436643262353536382D643862342D343064312D393930642D346261306264346666373666000000000
7	Client C: Locate (symmetric key by name) In: objectType = ‘00000002’, attributes={ Name={ Name=‘Key1’, NameType=‘00000001’} } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data:

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1 Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string) 42007801000000D042007701000000384200690100000020420 06A0200000004000000010000000042006B020000000400000000000000042000D020000000400000001000000042000F01000000884200 5C05000000040000000800000000420079010000007042000801000000284200 0A070000000B4F626A65637420547970650000000000042000B0500000004000000 0200000000420008010000003842000A07000000044E616D650000000042000B 0100000020420055070000000044B65793100000004200540500000004000000 0100000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED30 (Thu Nov 12 12:10:40 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f 42007B01000000B042007A01000000484200690100000020420 06A0200000004000000010000000042006B020000000400000000000000042009209000000080000000004AFBED3042000D020000000400000001000000042000F01000000584200 5C05000000040000000800000000420079F050000000400000000000000042007C0100000030420094070000002436643262353536382D643862342D343064312D393930642D346261306264346666373666000000000
8	Client C: Get (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	4ba0bd4ff76f 420078010000009042007701000000384200690100000020420 06A020000000400000001000000042006B020000000400000000000000042000D020000000400000001000000042000F01000000484200 5C050000000400000000A000000004200790100000030420094070000002436643262353536382D643862342D343064312D393930642D346261306264346666373666000000 Out: objectType = ‘00000002’, uuidKey, symmetricKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED30 (Thu Nov 12 12:10:40 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 7C228050CE4FADBFF51227C891117F9C Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128) 42007B010000012042007A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000042009209000000080000000 04AFBED3042000D020000000400000001000000042000F01000000C842005C05000000040000000A 0000000042007F050000000400000000000000042007C01000000A042005705000000040000000200000000420094070000002436643262353536382D643862342D343064312D393930642D346261306264346666373666000000042008F010000005842004001000000504200420500000004000000010000000042004501000000184200430800000107C228050CE4FADBFF51227C891117F9C4200280500000004000000030000000042002A020000000400000080000000
9	Client C: Get usage allocation In: uuidKey, UsageLimitsByteCount=’500’ Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f Tag: Usage Limits Byte Count (0x420096), Type: Big Integer (0x04), Data: 01F4 (500) 4200780100000A042007701000000384200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000042000D020000000400000001000000004200 0F01000005842005C050000000400000011000000004200 7901000000404200940700000024366432623535363 82D643862342D343064312D393930642D34626130626434666637366600000000420096040000000800000000000001F4 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED31 (Thu Nov 12 12:10:41 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Failed) Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x0000000C (Permission Denied) Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Unable to allocate requested amount 42007B01000000B842007A01000000484200690100000020420 06A020000000400000001000000004200 6B020000000400000000000000042009209000000080000000 04AFBED3142000D020000000400000001000000004200 0F01000000604200 5C050000000400000011000000004200 7F050000000400000001000000004200 7E050000000400000000C00000000420 07D0700000023556E61626C6520746F20616C6C6F6361746520726571756573746564206 16D6F756E740000000000
10	Client A: Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f 4200780100000090420077010000038420069010000002042006A020000000400000001000000004200 6B020000000400000000000000042000D020000000400000001000000004200 0F01000004842005C050000000400000014000000004200

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	790100000030420094070000002436643262353536382D643862342D343064312D393930642D34626130626434666637366600000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED31 (Thu Nov 12 12:10:41 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6d2b5568-d8b4-40d1-990d-4ba0bd4ff76f 42007B01000000B042007A01000000484200690100000020420 06A020000000400000001000000042006B020000000400000000000000042009209000000080000000 04AFBED3142000D020000000400000001000000042000F01000000584200 5C050000000400000014000000042007F050000000400000000000000042007C0100000030420094070000002436643262353536382D643862342D343064312D393930642D34626130626434666637366600000000

6 Key Interchange, Key Exchange

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

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

Time	Request/Response messages
0	Register (symmetric key) In: objectType = ‘00000002’, attributes={ CryptographicUsageMask=‘00000004’ }, foreignSymmetricKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000004 (Encrypt) Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 0123456789ABCDEF0123456789ABCDEF Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128) 42007801000001104200770100000038420069010000002042006A020000000400000001000000042006B02000000040 00000000000000042000D020000000400000001000000042000F01000000C842005C050000000400000030000000042 007901000000B042005705000000040000000200000000420091010000003842000801000000030420000A0700000018437 27970746F677261706869632055736167652040D61736B42000B020000000400000004000000042008F01000000584200 40010000005042004205000000040000000100000000420045010000001842004308000000100123456789ABCDEF01234 56789ABCDEF42002805000000040000000300000000420020A020000000400000080000000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED32 (Thu Nov 12 12:10:42 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7 42007B01000000B042007A01000000484200690100000020420 06A020000000400000001000000042006B02000000040 00000000000000042009209000000080000000004AFBED3242000D020000000400000001000000042000F010000005842 005C050000000400000003000000042007F050000000400000000000000042007C0100000030420094070000002436 6 53161356138332D383131332D343236302D623430642D393636663233316239316237000000000
1	Add attribute In: uuidKey, attribute={ x-provider='unknown' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-provider Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: unknown 4200780100000C04200770100000038420069010000002042006A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000007842005C050000000400000000D0000000042007901000000604200940700000024366531613561381332D383131332D343236302D623430642D3936366632333162393162370000000042000801000000284200A070000000A782D70726F766964657200000000000042000B0700000007756E6B6E6F776E00 Out: uuidKey, attribute={ x-provider='unknown' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED32 (Thu Nov 12 12:10:42 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-provider Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: unknown 42007B01000000E042007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000004AFBED3242000D020000000400000001000000042000F010000008842005C050000000400000000D0000000042007F050000000400000000000000000042007C0100000060420094070000002436653161356138332D383131332D343236302D623430642D3936366632333162393162370000000042000801000000284200A070000000A782D70726F766964657200000000000042000B0700000007756E6B6E6F776E00
2	Modify attribute In: uuidKey, attribute={ x-provider='third party' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-provider Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: third party 4200780100000C84200770100000038420069010000002042006A020000000400000001000000042006B02000000040000000000000042000D020000000400000001000000042000F010000008042005C050000000400000000E0000000420079010000006842009407000000243665316135613833 2D383131332D343236302D623430642D3936366632333162393162370000000042000801000000304200A070000000A782D70726F766964657200000000000042000B070000000B746869726420706172747900000000000 Out: uuidKey, attribute={ x-provider='third party' } Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED32 (Thu Nov 12 12:10:42 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-provider Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: third party 42007B01000000E842007A0100000048420069010000002042006A020000000400000001000000042006B02000000040000000000000042009209000000080000000 4AFBED3242000D020000000400000001000000042000F010000009042005C050000000400000000E0000000042007F050000000400000000000000000042007C0100000068420094070000002436653161356138332D383131332D343236302D623430642D3936366632333162393162370000000042000801000000304200A070000000A782D70726F766964657200000000000042000B070000000B746869726420706172747900000000000
3	Destroy (symmetric key) In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7 42007801000000904200770100000038420069010000002042006A020000000400000001000000004200 6B02000000040000000000000004200 0D020000000400000001000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002436653161356138332D383131332D343236302D623430642D3936366632333162393 1623700000000 Out: uuidKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED32 (Thu Nov 12 12:10:42 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6e1a5a83-8113-4260-b40d-966f231b91b7 42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200 6B02000000040000000000000004200920900000000800000000 4AFBED3242000D020000000400000001000000004200 0F010000005842005C050000000400000014000000004200 7F050000000400000000000000000042007C0100000030420094070000002436653161356138332D383131332D343236302D623430642D393636663233316239316237000000000

7 Vendor Extensions

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

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

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

Time	Client A
0	Create (symmetric key) In: objectType=’00000002’, attributes={ CryptographicAlgorithm=’AES’, CryptographicLength=’128’, CryptographicUsageMask=‘0000000C’ }, MessageExtension={ VendorIdentification=’Acme’,

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

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

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

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

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

8 Asymmetric keys

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

8.1 Use-case: Create a Key Pair

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

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

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Out: uuidPrivateKey, uuidPublicKey
1	Locate (Public Key) In: attributes={ objectType='PublicKey', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } } Out: uuidPublicKey
2	Locate (Private Key) In: attributes={ objectType='PrivateKey', Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } } Out: uuidPrivateKey
3	Destroy In: uuidPrivateKey Out: uuidPrivateKey
4	Destroy In: uuidPublicKey Out: uuidPublicKey

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

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

Time	Client A
0	Register (Private Key) In: objectType='00000004', attributes={ CryptographicUsageMask='0000000C' }, foreignPrivateKey Out: uuidPrivateKey
1	Register (Public Key) In: objectType='00000004', attributes={ CryptographicUsageMask='0000000C', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } }, foreignPublicKey Out: uuidPublicKey
2	Add attribute In: uuidPrivateKey, attribute={ Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } } Out: uuidPrivateKey, attribute={ Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } }
3	Locate (Public Key) In: attributes={ objectType='PublicKey', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } } Out: uuidPublicKey
4	Locate (Private Key) In: attributes={ objectType='PrivateKey', Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } }

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	Out: uuidPrivateKey
5	Destroy In: uuidPrivateKey Out: uuidPrivateKey
6	Destroy In: uuidPublicKey Out: uuidPublicKey

9 Key Roll-over

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

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

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

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

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	In: uuidKey Out: objectType = ‘00000002’, uuidKey, symmetricKey
6	Destroy In: uuidKey Out: uuidKey
7	Destroy In: uuidNewKey Out: uuidNewKey

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

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

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

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

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

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

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

Time	Client A
0	Create (symmetric key) In: objectType=’00000002’, attributes={ CryptographicAlgorithm=’AES’, CryptographicLength=’128’, CryptographicUsageMask=‘0000000C’, Name={ NameValue=‘rekeyKey’, NameType=’00000001’ }, ActivationDate=’2’ } Out: objectType=’00000002’, uuidKey
1	Get Attribute In: uuidKey, attributeName={‘State’} Out: uuidKey, attribute={ State=‘*Active*’ }
2	Revoke (symmetric key as compromised) In: uuidKey, RevocationReason=’00000002’, CompromiseOccurrenceDate=’6’ Out: uuidKey
3	Get Attribute In: uuidKey, attributeName={‘State’} Out: uuidKey, attribute={ State=‘*Compromised*’ }
4	Rekey In: uuidKey, offset=’0’ Out: uuidNewKey

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

5	Get Attribute In: uuidNewKey, attributeName={'State'} Out: uuidNewKey, attribute={ State='*Active*' }
6	Destroy In: uuidKey Out: uuidKey
7	Destroy In: uuidNewKey Out: uuidNewKey

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

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

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

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

6	Destroy In: uuidKey Out: uuidKey
7	Destroy In: uuidNewKey Out: uuidNewKey

9.5 Use-case: Obtain Lease for Expired Key

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

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

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

6	Locate (symmetric key) In: attributes={ Name={ NameValue='rekeyKey', NameType='00000001' } } Out: uuidNewKey	
7	Get (symmetric key) In: uuidNewKey Out: objectType = '00000002', uuidNewKey, newSymmetricKey	
8	Obtain Lease In: uuidNewKey Out: uuidNewKey, leaseTime, lastChangeDate	
9	Destroy In: uuidKey Out: uuidKey	
10	Destroy In: uuidNewKey Out: uuidNewKey	

10 Archival

These use-cases test archiving and locating keys using the off-line indicator. If the server performs the Archive and Recover operations asynchronously, the client Polls the server until the operations complete. The client indicates in the request that it supports asynchronous responses.

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

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

Time	Client A
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='archiveKey', NameType='00000001' } } Out: objectType='00000002', uuidKey
1	Locate In: attributes={ Name={ NameValue='archiveKey', NameType='00000001' } } Out: uuidKey
2	Get (symmetric key)

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

	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

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

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:

Gordon Arnold, IBM
Todd Arnold, IBM
Matthew Ball, Sun Microsystems
Elaine Barker, NIST
Peter Bartok, Venafi, Inc.
Mathias Björkqvist, IBM
Kevin Bocek, Thales e-Security
Kelley Burgin, National Security Agency
Jon Callas, PGP Corporation
Tom Clifford, Symantec Corp.
Graydon Dodson, Lexmark International Inc.
Chris Dunn, SafeNet, Inc.
Paul Earsy, SafeNet, Inc.
Stan Feather, HP
Indra Fitzgerald, HP
Alan Frindell, SafeNet, Inc.
Judith Furlong, EMC Corporation
Jonathan Geater, Thales e-Security
Robert Griffin, EMC Corporation
Robert Haas, IBM
Thomas Hardjono, M.I.T.
Marc Hocking, BeCrypt Ltd.
Larry Hofer, Emulex Corporation
Brandon Hoff, Emulex Corporation
Walt Hubis, LSI Corporation
Wyllys Ingersoll, Sun Microsystems
Jay Jacobs, Target Corporation
Glen Jaquette, IBM

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

Scott Kipp, Brocade Communications Systems, Inc.
David Lawson, Emulex Corporation
Robert Lockhart, Thales e-Security
Shyam Mankala, EMC Corporation
Marc Massar, Individual
Don McAlister, Cipheroptics
Hyrum Mills, Mitre Corporation
Landon Noll, Cisco Systems, Inc.
René Pawlitzek, IBM
Rob Philpott, EMC Corporation
Bruce Rich, IBM
Scott Rotondo, Sun Microsystems
Anil Saldhana, Red Hat
Subhash Sankuratripati, NetApp
Mark Schiller, HP
Jitendra Singh, Brocade Communications Systems, Inc.
Servesh Singh, EMC Corporation
Sandy Stewart, Sun Microsystems
Marcus Streets, Thales e-Security
Brett Thompson, SafeNet, Inc.
Benjamin Tomhave, Individual
Sean Turner, IECA, Inc.
Paul Turner, Venafi, Inc.
Marko Vukolic, IBM
Rod Wideman, Quantum Corporation
Steven Wierenga, HP
Peter Yee, EMC Corporation
Krishna Yellepeddy, IBM
Peter Zelechoski, Election Systems & Software

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

B. Revision History

Revision	Date	Editor	Changes Made
ed-0.98	2009-04-28	Mathias Björkqvist	Initial conversion of input document to OASIS format.
ed-0.98	2009-08-06	Mathias Björkqvist	Changes to layout and message content to reflect the recent changes to the KMIP specification, added descriptions to the use-cases for which they were missing.
ed-0.98	2009-09-28	Mathias Björkqvist	Updated messages and TTLV encodings to conform with KMIP specification ed-0.98 rev 17.
draft-01	2009-10-08	Mathias Björkqvist	Removed normative words “must”, “shall”, “required”, “will” and “can”; updated messages and TTLV encodings to conform to KMIP specification ed-0.98 rev 19; added normative references; added minor edits
draft-02	2009-10-15	Mathias Björkqvist	Replaced the TBDs, changed status to Committee Draft, changed use-cases to use protocol major version 1 and minor version 0
draft-03	2009-10-15	Mathias Björkqvist	Corrected names of TC chairs
draft-04	2009-11-05	Mathias Björkqvist	Added list of participants, added reference to Profiles document, line spacing change to list of original contributors, added related documents
cd-05	2009-11-06	Mathias Björkqvist	Changes to various naming aspects on front page and document footer. This is the tentative version for public review.
cd-06	2009-11-12	Mathias Björkqvist	Updated tags.

Copyright © OASIS® 2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.