Key Management Interoperability Protocol Use Cases Version 1.0

Committee Draft 07

Deleted: 06 / Public Review 02

17 February 2010

Deleted: 12 November 2009

Specification URIs:

This Version:

http://docs.oasis-open.org/kmip/usecases/v1.0/cd07/kmip-usecases-1.0-cd-07.html
http://docs.oasis-open.org/kmip/usecases/v1.0/cd07/kmip-usecases-1.0-cd-07.doc (Authoritative)
http://docs.oasis-open.org/kmip/usecases/v1.0/cd07/kmip-usecases-1.0-cd-07.pdf

Deleted: 06
Deleted: 06
Deleted: 06
Deleted: 06
Deleted: 06
Deleted: 06

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.

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

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

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

Notices

Copyright © OASIS® 2010. All Rights Reserved.

Deleted: 2009

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

Deleted: 1 Introduction . 5¶
1.1 Normative References . 5¶
2 Message exchange . 5¶
3 Centralized Management . 5¶
3.1 Basic functionality . 5¶
3.1.1 Use-case: Create / Destroy . 5¶
3.1.2 Use-case: Register / Create / Get attributes / Destroy . 8¶
3.1.3 Use-case: Create / Locate / Get / Destroy . 13¶
3.1.4 Use-case: Dual client use-case, ID Placeholder linked Locate & Get batch . 18¶
3.2 Use-case: Asynchronous Locate . 33¶
4 Key life cycle support . 43¶
4.1 Use-case: Revoke scenario . 43¶
5 Auditing and reporting . 60¶
5.1 Use-case: Get usage allocation scenario . 60¶
6 Key Interchange, Key Exchange . 72¶
6.1 Use-case: Import of a Third-party Key . 72¶
7 Vendor Extensions . 76¶
7.1 Use-case: Unrecognized Message Extension with Criticality Indicator false . 76¶
7.2 Use-case: Unrecognized Message Extension with Criticality Indicator true . 77¶
8 Asymmetric keys . 77¶
8.1 Use-case: Create a Key Pair . 77¶
8.2 Use-case: Register Both Halves of a Key Pair . 78¶
9 Key Roll-over . 79¶
9.1 Use-case: Create a Key, Re-key . 79¶
9.2 Use-case: Existing Key Expired, Re-key with Same lifecycle . 80¶
9.3 Use-case: Existing Key Compromised, Re-key with same lifecycle . 81¶
9.4 Use-case: Create key, Re-key with new lifecycle . 82¶
9.5 Use-case: Obtain Lease for Expired Key . 83¶
10 Archival . 84¶
10.1 Use-case: Create a Key, Archive and Recover it . 84¶
A. . Acknowledgments . 86¶
B. . Revision History . 88¶

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 Quality Assurance scenarios which would stress an implementation. The use-cases are based on v1.0 of the protocol.

Deleted: [

Deleted: KMIP-Spec

Deleted:]

Deleted: QA

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).

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

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

1.1 Normative References

[KMIP-Spec]	OASIS Draft, *Key Management Interoperability Specification v1.0,* Committee Draft, February 2010.
[KMIP-Prof]	OASIS Draft, *Key Management Interoperability Protocol Profiles v1,0,* Committee Draft, November 2009.

Deleted: 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 TLS/SSL transport as defined in **[KMIP-Spec]** and **[KMIP-Prof]**.

Deleted: http

Deleted: 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, template and secret data registration, attribute functionality, access methods, and batch operation.

Deleted: and

3.1.1 Use-case: Create / Destroy

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

Time	Request/Response messages
0	Create (symmetric key) In: objectType='00000002' (Symmetric Key), attributes={ CryptographicAlgorithm='00000003' (AES), CryptographicLength='128', CryptographicUsageMask='0000000C' }

```
Tag: Request Message (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)
```

```
42007801000001204200770100000038420069010000002042006A0200000004000000010000000042006B0200000004
0000000000000000042000D0200000004000000010000000042000F01000000D842005C0500000004000000010000000
42007901000000C04200570500000004000000020000000042009101000000A84200080100000030042000A0700000017
43727970746F677261706869632041 6C676F726974686D0042000B05000000040000000300000000420008010000003 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)
```

<table>
<tr>
<td></td>
<td>

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

```
42007B01000000C042007A0100000048420069010000002042006A02000000040000000100000000042006B0200000004
0000000000000000420092090000000800000000 4AFBE7C242000D0200000004000000010000000042000F0100000068
42005C0500000004000000010000000042007F0500000004000000000000000042007C01000000404200570500000004
000000020000000042009407000000246663383833336465 2D373064322D346563652D623036332D6665646533613363
3539666500000000
```

</td>
</tr>
<tr>
<td>1</td>
<td>

Destroy (symmetric key)

In: uuidKey

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

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004
0000000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000001400000000
4200790100000030420094070000002466633838333364652D373064322D346563652D623036332D6665646533613363
3539666500000000
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C3 (Thu Nov 12 
11:47:31 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
```

</td>
</tr>
</table>

<table>
<tr><td></td><td><pre>
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fc8833de-70d2-4ece-
b063-fede3a3c59fe

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004
00000000000000004200920900000008000000004AFBE7C342000D0200000004000000010000000042000F0100000058
42005C0500000004000000010000000042007F0500000004000000000000000042007C01000000304200940700000024
66633838333364652D373064322D346563652D623036332D66656465336133633539666500000000
</pre></td></tr>
</table>

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.

<table>
<tr><th>Time</th><th>Request/Response messages</th></tr>
<tr><td>0</td><td>Register (template)
In: objectType='00000007', attributes={ ObjectGroup='Group1', ApplicationSpecificInformation='ssl, www.example.com', ContactInformation='Joe', x-Purpose='demonstration', Name={ NameValue='Template1', NameType='00000001' } }
<pre>
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 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:
</pre></td></tr>
</table>

```
          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)
```

```
42007801000001C042007701000000384200690100000020420006A020000000400000001000000000042006B02000000040
000000000000000042000D02000000040000000100000000042000F01000001784200 5C05000000040000000300000000042
```

```
42007801000001C04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F010000017842005C0500000004000000030000000042
0079010000016042005705000000040000000600000000420091010000014842000801000000284200 0A070000000C4F6
26A6563742047726F7570000000000042000B07000000064772 6F757031000042000801000000584200 0A07000000204170
706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000B010000002842000307000000373736
C000000000042000207000000 0F7777772E6578616D706C652E636F6D00420008010000003042000A0700000013436F6E
7461637420496E666F726D6174696F6E00000000042000B07000000034A6F6500000000004200080100000030420000A0
700000009782D507572706F736500000000000000000042000B070000000D64656D6F6E7374726174696F6E00000042000801
000000404200 0A07000000044E616D650000000042000B0100000028420055070000000954656D706C617465310000000
00000000420054050000000040000000100000000
```

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
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004AFBE7C442000D0200000004000000010000000042000F010000005842
005C0500000004000000030000000042007F0500000004000000000000000042007C010000003042009407000000024613
66562626236662D346335342D346262622D616432392D626536626164346563616435000000000
```

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)
        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)
```

```
42007801000001504200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F01000001084200 5C0500000004000000010000000042
007901000000F04200570500000004000000020000000042009101000000D842005301000000284200550700000009546
56D706C61746531000000000000004200540500000004000000010000000042000801000000304200 0A07000000174372
7970746F6772617068696320416C676F726974686D0042000B050000000400000003000000004200080100000030420000
A07000000144372797074 6F6772617068696320 4C656E677468000000042000B020000000400000080000000000420008
010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000040000000
C00000000
```

Out: objectType=’00000002’, uuidKey

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

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004AFBE7C542000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F0500000004000000000000000042007C010000004042005705000000004000
00002000000004200940700000024363162313036313 42D643862352D343666392D386431372D32666136656131643734
376100000000
```

2

Get attributes

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

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-
2fa6ea1d747a
      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
```

```
42007801000001084200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000000C042005C05000000040000000B0000000042
007901000000A8420094070000002436316231303631342D643862352D343666392D386431372D3266613665613164373
4376100000000042000A070000000C4F626A6563742047726F75700000000042000A07000000204170706C69636174696F
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
```

```
42007B01000001B042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000042009209000000080000000004AFBE7C642000D0200000004000000010000000042000F010000015842
005C05000000040000000B000000042007F050000000400000000000000000042007C010000013042009407000000024363
16231303631342D643862352D343666392D386431372D32666136656131643734376100000000042000801000000284200
0A070000000C4F626A6563742047726F7570000000000042000B070000000647726F75703100004200080100000058420000
A07000000204170706C69636174696F6E20537065636966696320496E666F726D6174696F6E42000B010000002842000 3
070000000373736C00000000000420002070000000F7777772E6578616D706C652E636F6D0042000801000000003042000A0
700000013436F6E7461637420496E666F726D6174696F6E000000000042000B07000000034A6F650000000000042000801
0000003042000A0700000009782D507572706F7365000000000000000042000B070000000D64656D6F6E7374726174696F6
E000000
```

3

Destroy (symmetric key)

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-
2fa6ea1d747a
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
0000000000000000042000D02000000040000000100000000042000F01000000484200 5C050000000400000014000000042
00790100000030420094070000002436316231303631342D643862352D343666392D386431372D32666136656131643734373
4376100000000
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C6 (Thu Nov 12
11:47:34 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 61b10614-d8b5-46f9-8d17-
2fa6ea1d747a
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
```

	00000000000000042009209000000080000000004AFBE7C642000D020000000400000001000000000042000F010000005842 005C050000000400000014000000004200 7F050000000400000000000000000042007C010000003042009407000000024363 16231303631342D643862352D343666392D386431372D32666136656131643734376100000000

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)
	      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
	
	420078010000009042007701000000384200690100000020420 06A0200000004000000010000000042006B020000000040
	000000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000140000000042
	0079010000003042009407000000246136656262623666 2D346335342D346262622D616432392D62653662616434656361
	1643500000000
	
	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
	
	42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000040
	00000000000000042009209000000080000000004AFBE7C642000D020000000400000001000000000042000F010000005842
	005C05000000040000001400000000 42007F050000000400000000000000000042007C010000003042009407000000024613
	66562626236662D346335342D346262622D616432392D62653662616434656361643500000000

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.

<table>
<tr><th>Time</th><th>Request/Response messages</th></tr>
<tr><td>0</td><td>

Create (symmetric key)

In: objectType = ‘00000002’, attributes={ Name={ NameValue=‘Key1’, NameType=’00000001’ }, CryptographicAlgorithm=’DES’, CryptographicLength=’56’, CryptographicUsageMask=‘0000000C’, ContactInformation=’Joe’ }

```
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: 0x00000002 (3DES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x000000A8 (168)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt,
Decrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe
```

```
42007801000001984200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F01000001504200 5C0500000004000000010000000042
00790100000138420057050000000400000002000000004200910100000120420008010000003842000A07000000044E6
16D650000000042000B010000002042005507000000044B657931000000004200540500000004000000010000000042 00
0801000000304200 0A070000001743727970746F6772617068696320416C676F726974686D0042000B050000000400000
002000000004200080100000030 42000A0700000014437279707 46F6772617068696320 4C656E677468000000000042000B
02000000040000 00A80000000042000801000000304200 0A0700000018437279707 46F677261706869632055736167652
04D61736B42000B02000000040000000C0000000042000801000000304200 0A0700000013436F6E7461637420496E666F
726D6174696F6E0000000000042000B07000000034A6F650000000000
```

</td></tr>
</table>

Deleted: 1

Deleted: 3

Deleted: 56

Deleted: 1

Deleted: 3

Out: objectType = ‘00000002’, uuidKey

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

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004AFBE7C742000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F0500000004000000000000000042007C010000004042005705000000004000
00002000000004200940700000024316564323865613 52D326233312D343134352D626366322D333664303735366433338
393000000000
```

1 Locate (symmetric key)

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

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

```
42007801000000D0420077010000003842006901000000 2042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F010000008842005C050000000400000008000000042
00790100000070420008010000002842000A070000000B4F626A6563742054797065000000000042000B050000000040 00
00002000000004200080100000038 42000A07000000044E616D650000000042000B010000002042005507000000044B65
793100000000420054050000000400000001 00000000
```

Out: uuidKey

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

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004AFBE7C842000D0200000004000000010000000042000F010000005842
005C0500000004000000080000000042007F0500000004000000000000000042007C010000003042009407000000024316
5643238656135 2D326233312D343134352D626366322D3336643037353664333839300000000000
```

2 Get (symmetric key)

In: uuidKey

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

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000A0000000042
00790100000030420094070000002431656432386561352D326233312D343134352D626366322D3336643037353664333
8393000000000
```

Out: objectType = ‘00000002’, uuidKey, symmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBE7C8 (Thu Nov 12
11:47:36 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1ed28ea5-2b31-4145-bcf2-
36d0756d3890
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data:
C8E51523F73D6EE9F40EAB7CD06825499D8C0BD0739E1046
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000002
(3DES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x000000A8 (168)

42007B010000012842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004AFBE7C842000D0200000004000000010000000042000F01000000D042
005C050000000400000000A0000000042007F050000000400000000000000000042007C01000000A8420057050000000400
00002000000004200940700000024316564323865613520326233312D343134352D626366322D333664303735366433338
393000000000042008F010000006042004001000000584200420500000004000000010000000042004501000000020420004
308000000018C8E51523F73D6EE9F40EAB7CD06825499D8C0BD0739E1046420028050000000400000002000000042002A
020000000400000A800000000
```

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


42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000140000000042
00790100000030420094070000002431656432386561352D326233312D343134352D626366322D3336643037353664333
8393000000000
```

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)
```

Deleted: 4564A76DF1A77662

Deleted: 1

Deleted: 3

Deleted: 56

Deleted: 1

Deleted: C

Deleted: 9

Deleted: 5

Deleted: 4

Deleted: 1

Deleted: 084564A76DF1A77662420028050000000400000001000000042002A02000000040000003800000000

```
      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
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004AFBE7C842000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F0500000004000000000000000042007C010000003042009407000000024316
56432386561352D326233312D343134352D626366322D3336643037353664333839300000000
```

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
```

```
42007801000000B84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000007042005C050000000400000008000000042
00790100000058420008010000005042000A0700000011556E69717565204964656E7469666965720000000000000000420
00B0700000002431656432386561352D326233312D343134352D626366322D3336643037353664333839300000000
```

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
```

```
42007B0100000008042007A010000000484200690100000002042006A02000000004000000010000000042006B02000000040
0000000000000000420092090000000080000000004AFBE7C842000D02000000004000000010000000042000F010000002842
005C05000000004000000080000000042007F05000000004000000000000000042007C0100000000
```

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

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

This use-case demonstrates the fact that 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.

Deleted: 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)
```

```
420078010000013042007701000000384200690100000020420006A02000000040000000100000000420006B02000000040
0000000000000042000D0200000004000000010000000042000F01000000E842005C050000000400000003000000042
007901000000D042005705000000040000000600000000420091010000000B842000801000000304200A07000000017437
27970746F67726170686963416C676F726974686D0042000B05000000040000000300000000420008010000003042000
0A07000000144372797074F67726170686963204C656E677468000000042000B0200000004000000080000000042000
8010000004042000A07000000044E616D650000000042000B0100000028420055070000000954656D706C617465310000
000000000042005405000000040000000100000000
```

Out: uuidTemplate

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

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
00000000000000042009209000000080000000004AFBED2142000D0200000004000000010000000042000F010000005842
005C050000000400000003000000042007F0500000004000000000000000042007C010000003042009407000000024343
56438363239612D396164312D343162332D396430392D393431663261353935646133300000000
```

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)
        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
```

```
42007801000001584200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000011042005C0500000004000000010000000042
007901000000F842005705000000040000000200000000420091010000000E042005301000000284200550700000009546
56D706C617465310000000000000042005405000000040000000100000000420008010000003842000A07000000044E61
6D650000000042000B010000002042005507000000044B6579310000000042005405000000040000000100000000042000
8010000003042000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000
0400000000420008010000003042000A0700000013436F6E7461637420496E666F726D6174696F6E0000000000042000B0
700000003466F6F0000000000
```

Out: objectType='00000002', uuidKey

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

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000004200920900000008000000004AFBED2342000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F0500000004000000000000000042007C010000004042005705000000040000
0002000000004200940700000024306133336538336520356237612D343836352D393634612D38643163336262663961
653300000000
```

2 Client B:

Locate and Get (symmetric key by name)

In (header): batchOrderOption='TRUE'

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

In: <empty Get payload>

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

```
42007801000001204200770100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420010060000000800000000000000014200D02000000040000000200000000042000F010000009842
005C050000000400000008000000004200930800000080E9E1875336E415E4200790100000070420008010000002842
000A070000000B4F626A656374205479706500000000042000B050000000400000002000000004200080100000384200
0A07000000044E616D65000000000042000B010000002042005507000000044B657931000000004200540500000000400000
0010000000042000F010000002842005C050000000400000000A00000000420093080000008CFEF21DDDF1CF5E3420079
0100000000
```

Out: uuidKey

Out: objectType='00000002', uuidKey, symmetricKey

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

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

```
42007B01000001A042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004AFBED2442000D0200000004000000020000000042000F010000006842
005C0500000004000000080000000042009308000000080E9E1875336E415E42007F0500000004000000000000000000420
07C01000000304200940700000024306133336538336523D356237612D343836352D393634612D38643163336262663961
65330000000042000F01000000D842005C05000000040000000A00000000420093080000008CFEF21DDDF1CF5E342007
F050000000400000000000000042007C01000000A04200570500000004000000020000000042009407000000024306133
33653833652D356237612D343836352D393634612D38643163336262663961653300000000042008F01000000584200400
10000005042004205000000040000000100000000420045010000001842004308000000010755D03C639648FB5828D5F1C
C9FE9B57420028050000000400000003000000042002A020000000400000008000000000
```

3

Client B:

Get attribute list

In: uuidKey

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

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000000484200 5C0500000004000000 0C0000000042
00790100000030420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663 96
1653300000000
```

Out: uuidKey, attributes={ * }

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

```
42007B01000001C842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004AFBED2442000D0200000004000000010000000042000F010000017042
005C05000000040000000C0000000042007F05000000040000000000000000042007C01000001484200940700000024306
13333653833652D356237612D343836352D393634612D386431633362626639616533000000000042000A07000000144372
7970746F6772617068696320 4C656E677468000000000042000A07000000174372797074 6F6772617068696320416C676F7
26974686D0042000A070000000553746174650000000042000A070000000644696765737400000042000A070000000C496E69
7469616C2044617465000000000042000A0700000011556E69717565204964656E7469666965720000000000000042000A0
7000000044E616D650000000042000A070000001843727970746F6772617068696320557361676520 4D61736B42000A07
0000000B4F626A6563742054797065000000000042000A070000000013436F6E7461637420496E666F726D6174696F6E000
000000042000A07000000104C61737420436861 6E67652044617465
```

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
```

<table>
<tr>
<td></td>
<td>

```
42007801000000C042007701000000384200690100000020042006A02000000040000000100000000042006B02000000040
0000000000000000042000D0200000004000000010000000042000F010000007842005C050000000400000000B0000000042
0079010000006042009407000000243061333653833652D356237612D343836352D393634612D3864316333626266396
16533000000000042000A07000000044E616D650000000042000A0700000013436F6E7461637420496E666F726D6174696F
6E0000000000
```

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

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED24 (Thu Nov 12
12:10:28 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-
8d1c3bbf9ae3
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Foo
```

```
42007B010000012842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004AFBED2442000D0200000004000000010000000042000F01000000D042
005C050000000400000000B0000000042007F0500000004000000000000000042007C01000000A842009407000000024306
1333653833652D356237612D343836352D393634612D3864316333626266396165330000000042000801000000384200
0A07000000044E616D650000000042000B01000000204200550700000044B6579310000000042005405000000040000
00100000000420008010000003042000A0700000013436F6E7461637420496E666F726D6174696F6E000000000042000B
0700000003466F6F0000000000
```

</td>
</tr>
<tr>
<td>5</td>
<td>

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)
```

</td>
</tr>
</table>

```
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7A92DDA525EB158A
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value1
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7230F6E4D3BEA249
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value2
```

```
42007801000001604200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000042000D0200000004000000020000000042000F010000008842005C05000000040000000D0000000042
009308000000087A92DDA525EB158A4200790100000060420094070000002430613333653833652D356237612D3438363
52D393634612D38643163336262663961653300000000420008010000002842000A070000000C782D6174747269627574
65310000000042000B070000000656616C756531000042000F010000008842005C05000000040000000D0000000042009
308000000087230F6E4D3BEA2494200790100000060420094070000002430613333653833652D356237612D343836352D
393634612D38643163336262663961653300000000420008010000002842000A070000000C782D6174747269627574653
200000000042000B070000000656616C7565320000
```

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

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

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

	Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-8d1c3bbf9ae3 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2 Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Value2 42007B010000019042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040 000000000000000420092090000000800000004AFBED2542000D0200000004000000020000000042000F010000009842 005C0500000004000000D00000000420093080000000087A92DDA525EB158A42007F0500000004000000000000000420 07C0100000060420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961 6533000000000420008010000002842000A070000000C782D617474726962757465310000000042000B070000000656616 C756531000042000F010000009842005C0500000004000000D000000004200930800000000087230F6E4D3BEA24942007F 0500000004000000000000000042007C0100000060420094070000002430613333653833652D356237612D343836352D3 93634612D38643163336262663961653300000000042000801000000002842000A070000000C782D6174747269627574653 2 000000042000B070000000656616C7565320000
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 420078010000017042007701000000384200690100000020420006A0200000004000000010000000042006B02000000040 000000000000000042000D0200000004000000020000000042000F010000009042005C0500000004000000E0000000042 00930800000008BA3EA60548ECB69942007901000000684200940700000024306133336538336352D356237612D3438363 52D393634612D38643163336262663961653300000000042000801000000003042000A070000000C782D6174747269627574 653100000000042000B070000000E4D6F646966696564566616C756531000042000F010000009042005C050000000400000 00E0000000042009308000000008321984E716274A3D42007901000000684200940700000024306133336538336 52D3562

```
37612D343836352D393634612D38643163336262663961653300000000420008010000003042000A070000000C782D617
474726962757465320000000042000B070000000E4D6F646966696564456616C7565320000
```

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

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

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED26 (Thu Nov 12
12:10:30 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BA3EA60548ECB699
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-
8d1c3bbf9ae3
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 321984E716274A3D
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0a33e83e-5b7a-4865-964a-
8d1c3bbf9ae3
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2
```

```
42007B01000001A042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004AFBED2642000D0200000004000000020000000042000F01000000A042
005C05000000040000000E0000000042009308000000008BA3EA60548ECB69942007F050000000400000000000000000420
07C0100000068420094070000002430613333653833652D356237612D343836352D393634612D386431633362626663961
653300000000420008010000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F6
4696669656456616C75653100000042000F01000000A042005C05000000040000000E00000000420093080000000008321984
E716274A3D42007F0500000004000000000000000042007C0100000068420094070000002430613333653833652D35623
7612D343836352D393634612D38643163336262663961653300000000420008010000003042000A070000000C782D6174
74726962757465320000000042000B070000000E4D6F646966696564456616C7565320000
```

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
      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
```

```
42007801000001304200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000020000000042000F010000007042005C05000000040000000F0000000042
00930800000008D5C6DF842DAEECD842007901000000484200940700000024306133336538336 52D356237612D3438363
52D393634612D38643163336262663961653300000000 42000A070000000C782D617474726962757465310000000042 00
0F010000007042005C05000000040000000F00000000420093080000000857 2D4F0D433DAB104200790100000048 42009
40700000024306133336538336 52D356237612D343836352D393634612D3864316333626266396165330000000042000A
070000000C782D6174747269627574653200000000
```

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 42007B01000001A042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040 00000000000000042009209000000080000000004AFBED2642000D0200000004000000020000000042000F01000000A042 005C0500000004000000F000000004200930800000008D5C6DF842DAEECD842007F0500000004000000000000000000420 07C0100000068420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961 653300000000420008010000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F6 4696669656456616C75653100000042000F01000000A042005C0500000004000000F00000000420093080000008572D4F 0D433DAB1042007F05000000040000000000000000042007C0100000068420094070000002430613333653833652D35623 7612D343836352D393634612D386431633362626639616533000000004200080100000030420000A070000000C782D6174 747269627574653200000000042000B070000000E4D6F646966696564456616C7565320000
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 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040 0000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000000042 00790100000030420094070000002430613333653833652D356237612D343836352D393634612D38643163336262663961 653300000000 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:

<table>
<tr>
<td></td>
<td>

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

42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420006B02000000040
00000000000000004200920900000008000000004AFBED2742000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F0500000004000000000000000042007C01000000304200940700000024306
13333653833652D356237612D343836352D393634612D386431633362626639616533000000000
```

</td>
</tr>
<tr>
<td>9</td>
<td>

Client A:

Get (symmetric key)

In: uuidKey

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

42007801000000904200770100000038420069010000002042006A02000000040000000100000000420006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000000A0000000042
00790100000030420094070000002430613333653833652D356237612D343836352D393634612D3864316333626266396
1653300000000
```

Out: Operation Failed, Item Not Found

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

42007B01000000A842007A0100000048420069010000002042006A02000000040000000100000000420006B02000000040
00000000000000004200920900000008000000004AFBED2742000D0200000004000000010000000042000F010000005042
005C0500000004000000A0000000042007F0500000004000000010000000042007E05000000040000000100000000420
07D07000000154F626A65637420646F6573206E6F742065786973740000000
```

</td>
</tr>
<tr>
<td>10</td>
<td>

Client A:

Destroy (template)

</td>
</tr>
</table>

Deleted: No Cryptographic Object found with given Unique Identifier

Deleted: D0

Deleted: 78

Deleted: 3A4E6F2043727970746F67726170686963204F626A65637420666F756E64207769746820676976656E20556E69717565204964656E74696669657200000000000000

	In: uuidTemplate
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 45d8629a-9ad1-41b3-9d09-941f2a595da3
	
	42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000000000000042000D0200000004000000010000000042000F01000000484200 5C05000000040000001400000000420079010000003042009407000000243435643836323961 2D396164312D343162332D396430392D3934316632613539356461330000000 0
	
	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
	
	42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000000000000004200920900000008000000004AFBED2742000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000000000000042007C010000003042009407000000243435643836323961 2D396164312D343162332D396430392D39343166326135393564613300000000

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

```
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 45d8629a-9ad1-41b3-9d09-
941f2a595da3

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000000484200 5C0500000004000000000A0000000042
007901000000304200940700000024343564383632396 12D396164312D343162332D396430392D393431663261353935 6
4613300000000
```

Out: Operation Failed, Item Not Found

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

42007B01000000D042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004AFBED2742000D0200000004000000010000000042000F010000007842
005C0500000004000000000A0000000042007F0500000004000000010000000042007E0500000004000000010000000420
07D070000003A4E6F2043727970746F67726170686963204F626A65637420666F756E6420776974682067697665 6E2055
6E697175652049646 56E746966696572000000000000
```

3.1.5 Use-case: Register / Destroy Secret Data

Formatted: Bullets and Numbering

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

Time	Request/Response messages

0	Register (secret data)
	In: objectType='00000007' (Secret Data), attributes={ CryptographicUsageMask='00000002' }
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)

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

```
420078010000010042007701000000384200690100000020042006A0200000004000000010000000042006B0200000004
00000000000000042000D020000000400000001000000042000F01000000B842005C050000000400000003000000000
42007901000000A0420057050000000400000007000000004200910100000038420008010000003042000A0700000018
43727970746F6772617068696320557361676520D61736B42000B020000000400000002000000004200850100000048
4200860500000004000000010000000042004001000000304200420500000004000000020000000042004501000000018
420043080000000E53656372657450617373776F72640000
```

Out: uuidObject

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

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004
000000000000000042009209000000080000000004B7924D142000D0200000004000000010000000042000F0100000058
42005C05000000040000000300000000042007F050000000400000000000000000042007C010000003042009407000000024
3339363232636332D653564342D346461392D396631302D33626466363462306537363000000000
```

1

Destroy (secret data)

In: uuidObject

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

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004
00000000000000004200 0D02000000040000000100000000 42000F01000000484200 5C050000000400000014000000000
420079010000003042009407000000243339363232636332 2D653564342D346461392D396631302D3362646636346230
653736300000000
```

Out: uuidKey

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

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004
000000000000000042009209000000080000000004B7924D142000D0200000004000000010000000042000F0100000058
42005C0500000004000000140000000042007F0500000004000000000000000042007C010000003042009407000000024
3339363232636332 2D653564342D346461392D396631302D33626466363462306537363000000000
```

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 to 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

Deleted: 3.1.4

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’ }

```
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
```

```
42007801000001904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000014842005C0500000004000000010000000042
00790100000130420057050000000400000002000000004200910100000118420008010000003042000A0700000017437
27970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000
0A070000001443727970746F6772617068696320416C656E67746800000000042000B02000000040000000800000000420000
80100000038420000A07000000044E616D650000000042000B0100000020420055070000000044B65793100000000420054
0500000004000000010000000042000801000000304200A0700000018437279707406F6772617068696320557361676520
4D61736B42000B0200000004000000040000000042000801000000284200A070000000C4F626A6563742047726F7570
0000000042000B070000000647726F7570310000
```

<table>
<tr>
<td></td>
<td>

Out: objectType = ‘00000002’, uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED28 (Thu Nov 12
12:10:32 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 95a0e6b3-8edc-4ffb-a88e-
e164539dbcca
```

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000000 4AFBED2842000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F0500000004000000000000000042007C01000000404200570500000004000
0000200000000420094070000002439356130653662332D386564632D346666622D613838652D65313634353339646263
636100000000
```

</td>
</tr>
<tr>
<td>1</td>
<td>

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)
```

</td>
</tr>
</table>

	42007801000000E04200770100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000000420007060000000080000000000000001420000D0200000004000000010000000042000F010000008842005C050000000400000008000000004200790100000070420008010000002842000A070000000B4F626A65637420547970650000000000042000B050000000400000002000000004200080100000038420000A07000000044E616D65000000004200 0B010000002042005507000000044B657931000000004200540500000004000000010000000 Out: asyncCorrValue1 Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED28 (Thu Nov 12 12:10:32 CET 2009) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Pending) Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 130BC369AF005A7F 42007B010000008842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000000420092090000000800000004AFBED2842000D0200000004000000010000000042000F0100000030420 05C0500000004000000080000000042007F05000000040000000200000000420006080000000813 0BC369AF005A7F
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 420078010000007042007701000000384200690100000002042006A0200000004000000010000000042006B0200000004000000000000000042000D0200000004000000010000000042000F010000002842005C05000000040000001A000000004200790100000010420006080000000813 0BC369AF005A7F 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
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004AFBED2842000D0200000004000000010000000042000F010000005842
005C05000000040000000800000000042007F0500000004000000000000000042007C010000003042009407000000024393
56130653662332D386564632D346666622D613838652D65313634353339646263636100000000
```

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
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000A0000000042
0079010000003042009407000000243935613065366232D386564632D346666622D613838652D65313634353339646263
3636100000000
```

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)
```

```
42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000000004AFBED2942000D0200000004000000010000000042000F01000000C842
005C05000000040000000A0000000042007F0500000004000000000000000042007C01000000A04200570500000004000
0000200000000420094070000002439356130653662332D386564632D346666622D613838652D65313634353339646263
6361000000000042008F01000000584200400100000050420042050000000400000001000000004200450100000018420043
0800000010BEF01F82DFB4682A01C2A08413834AAB420028050000000400000003000000004 2002A02000000040000000
8000000000
```

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
```

```
42007801000000D042007701000000484200690100000020 42006A0200000004000000010000000042006B02000000040
00000000000000042000706000000080000000000000000142000D0200000004000000010000000042000F010000007842
005C0500000004000000080000000042007901000000604200080100000028420000A070000000B4F626A6563742054797
065000000000042000B05000000040000000200000000420008010000002842000A070000000C4F626A656374204772 6F
75700000000042000B070000000647726F7570310000
```

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
```

```
42007B010000008842007A010000004842006901000000204 2006A020000000400000001000000004 2006B02000000040
```

```
42007B010000008842007A01000000484200690100000020420 06A020000000400000001000000004 2006B02000000040
```

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
```

```
42007801000000704200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F010000002842005C05000000040000001A0000000042
0079010000001042000608000000000848D43C207CD1FB3A
```

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
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004AFBED2942000D0200000004000000010000000042000F010000005842
005C0500000004000000080000000042007F0500000004000000000000000042007C01000000304200940700000024393
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:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), 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
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A0000000042
00790100000030420094070000002439356130653662332D386564632D346666622D613838652D6531363435333964626
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)
```

```
42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000000 4AFBED2942000D0200000004000000010000000042000F01000000C842
005C05000000040000000A0000000042007F0500000004000000000000000042007C01000000A04200570500000004000
00002000000004200940700000024393561306536623 32D386564632D346666622D613838652D65313634353339646263
6361000000000042008F0100000058420040010000005042004205000000040000000100000000420045010000001842004
30800000010BEF01F82DFB4682A01C2A08413834AAB4200280500000004000000030000000042002A0200000004000000
8000000000
```

7

Client B:

Locate (symmetric key by name)

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

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric
Key)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Name Value (0x420055), Type: Text String (0x07), Data: Key1
          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
```

```
42007801000000E042007701000000484200690100000020 42006A0200000004000000010000000042006B02000000040
000000000000000420007060000000800000000000000014 2000D0200000004000000010000000042000F0100000008842
005C0500000004000000080000000042007901000000704200080100000028 42000A070000000B4F626A6563742054797
0650000000000 42000B0500000004000000020000000042000801000000384 2000A07000000044E616D650000000004200
0B01000000204200550700000004 4B65793100000000420054050000000400000001 00000000
```

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 42007B010000008842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040 000000000000000420092090000000080000000004AFBED2942000D0200000004000000010000000042000F010000003042 005C0500000004000000080000000042007F0500000004000000020000000042000608000000084D6BBFC35FE57FBA
8	Client B: Cancel In: asyncCorrValue5 Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000019 (Cancel) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 4D6BBFC35FE57FBA 42007801000000704200770100000038420069010000002042006A0200000004000000010000000042006B02000000040 00000000000000042000D0200000004000000010000000042000F010000002842005C05000000040000001900000000042 00790100000010420006080000000084D6BBFC35FE57FBA 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) 42007B01000000A042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040 000000000000000420092090000000080000000004AFBED2942000D0200000004000000010000000042000F010000004842 005C0500000004000000190000000042007F0500000004000000000000000042007C0100000020420006080000000084D6 BBFC35FE57FBA42001205000000040000000100000000

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)`
	`  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`
	
	`42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040`
	`000000000000000042000D0200000004000000010000000042000F01000000484 2005C050000000400000014000000000 42`
	`00790100000030420094070000002439356130653662332D386564632D346666622D613838652D6531363435333964626`
	`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`
	
	`42007B01000000B042007A01000000484200690100000020 42006A0200000004000000010000000042006B02000000040`
	`00000000000000042009209000000080000000004AFBED2A42000D0200000004000000010000000042000F0100000058 42`
	`005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002439 3`
	`56130653662332D386564632D346666622D613838652D65313634353339646263636100000000`

* = 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.

<table>
<tr><th>Time</th><th>Client</th></tr>
<tr><td>0</td><td>Client A:
Create (symmetric key)
In: objectType = ‘00000002’, attributes={ CryptographicAlgorithm=’AES’, CryptographicLength=’128’, Name={ NameValue=‘Key1’, NameType=’00000001’ }, CryptographicUsageMask=‘00000004’ }
<pre>
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 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)

4200780100000160420077010000003842006901000000204200 6A02000000040000000100000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F0100000118420 05C0500000004000000010000000042
0079010000010042005705000000040000000200000000420091010000000E8420008010000003042000A0700000017437
27970746F6772617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042 00
0A070000001443727970746F6772617068696320 4C656E67746800000000042000B020000000400000080000000042000
8010000003842000A07000000044E616D650000000042000B010000002042005507000000044B65793100000000420054
</pre></td></tr>
</table>

Deleted: A

```
0500000004000000010000000042000801000000030420000A0700000001843727970746F677261706869632055736167652
04D61736B42000B020000000040000000400000000
```

Out: objectType = ‘00000002’, uuidKey

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

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004AFBED2B42000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F0500000004000000000000000042007C010000004042005705000000004000
0000200000000420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616164
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
```

```
42007801000000A0420077010000003842006901000000202042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B0000000042
0079010000004042009407000000243231643238623861 2D303664662D343363302D623732662D326131363133363333616
46139000000000042000A070000000553746174650000000
```

Out: uuidKey, attribute={ State=‘00000001’ }

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

42007B01000000D842007A0100000048420069010000002042006A02000000040000000100000000420006B02000000040
00000000000000042009209000000080000000004AFBED2B42000D0200000004000000010000000042000F010000008042
005C05000000040000000B00000000042007F05000000040000000000000000042007C010000005842009407000000024323
16432386238612D303664662D343363302D623732662D326131363136333361646139000000000420008010000000204200
0A07000000055374617465000000042000B050000000400000001000000000
```

2

Client A:

Activate

In: uuidKey

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

42007801000000904200770100000038420069010000002042006A02000000040000000100000000420006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000120000000042
00790100000030420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616
4613900000000
```

Out: uuidKey

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

Deleted: Add attribute

Deleted: , attribute={ ActivationDate='2'}

Formatted: Font: Italic

Deleted:
```
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)¶
¶
4200780100000000C0420077010000
0038420069010000002042006A02
00000004000000010000000004200
6B020000000400000000000000000
42000D020000000040000000010000
000042000F010000007842005C05
00000004000000D000000004200
790100000060420094070000000024
32316432386238612D303664662D
343363302D623732662D32613136
313633333616461390000000004200
0801000000002842000A070000000F
416374697661746966F6E204
```
... [1]

Deleted: , attribute={ ActivationDate='2'}

Formatted: Font: Italic

```
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12
12:10:35 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000012 (Activate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-
2a161633ada9

42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420 06B02000000040
00000000000000004200920900000008000000004AFBED2B42000D0200000004000000010000000042000F010000005842
005C0500000004000000120000000042007F0500000004000000000000000042007C010000003042009407000000024323
16432386238612D303664662D343363302D623732662D32613136313633336164613900000000
```

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

42007801000000A0420077010000003842006901000000204200 6A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B0000000042
00790100000040420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616
4613900000000042000A07000000055374617465000000
```

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-
```

Deleted: 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-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)¶
¶
42007B01000000E042007A010000004842006901000000 2042006A0200000004000000010000000042006B02000000040000000000000000420092090000000800000000 4AFBED2B42000D02000000040000000100000000 42000F01000000884200 5C0500000004000000 0D0000000042007F050000000400000000000000000042007C01000000604200940700000024323164323862 38612D303664662D343363302D623732662D32613136313633336164613900000000042000801000000028420
```

... [2]

```
2a161633ada9
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active)


42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000000 4AFBED2B42000D0200000004000000010000000042000F010000008042
005C0500000004000000 0B0000000042007F0500000004000000000000000042007C0100000058420094070000002 4323
16432386238612D303664662D343363302D623732662D326131363136333361646139000000000042000801000000204200
0A0700000005537461746500000042000B05000000040000000200000000
```

4

Client B:

Locate (symmetric key by name)

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

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


42007801000000D042007701000000384200690100000020 42006A0200000004000000010000000042006B02000000040
000000000000000 42000D0200000004000000010000000042000F010000008842005C0500000004000000080000000042
00790100000070420008010000002842000A070000000B4F626A656374205479706500000000000042000B05000000040 00
00002000000000420008010000003842000A07000000044E616D650000000042000B010000002042005507000000044B65
79310000000042005405000000040000000100000000
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12
12:10:35 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-
2a161633ada9
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
0000000000000004200920900000008000000004AFBED2B42000D0200000004000000010000000042000F010000005842
005C0500000004000000080000000042007F05000000040000000000000000042007C0100000030420094070000024323
16432386238612D303664662D343363302D623732662D3261313631363333616461390000000
```

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
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A0000000042
0079010000003042009407000000243231643238623861 2D303664662D343363302D623732662D326131363136333361 6
4613900000000
```

Out: objectType = ‘00000002’, uuidKey, symmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2B (Thu Nov 12
12:10:35 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-
2a161633ada9
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data:
EF7833AB15F5A1EE5874BC0D9BBC4BE7
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003
(AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)


42007B010000012042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
```

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)


42007801000000B84200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
0000000000000000042000D0200000004000000010000000042000F010000007042005C050000000400000013000000042
00790100000058420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616
461390000000042008101000000104200820500000004000000020000000042002109000000080000000000000006
```

Out: uuidKey

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

	Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-2a161633ada9 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000000000000420092090000000800000004AFBED2B42000D0200000004000000010000000042000F010000005842005C0500000004000000130000000042007F0500000004000000000000000042007C010000003042009407000000243231643238623861 2D303664662D343363302D623732662D326131363136333361646139000000000
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 420078010000000A04200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B0000000042007901000000404200940700000024323164323862386 12D303664662D343363302D623732662D32613136313633336164613900000000042000A07000000055374617465000000 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)

```
42007B01000000D842007A0100000048420069010000002042006A02000000040000000100000000420006B02000000040
000000000000000042009209000000080000000004AFBED2C42000D0200000004000000010000000042000F010000008042
005C0500000004000000B0000000042007F05000000040000000000000000042007C010000005842009407000000024323
16432386238612D303664662D343363302D623732662D326131363136333361646139000000000420008010000002042000
0A0700000005537461746500000042000B050000000400000004000000000
```

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
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000000484200 5C050000000400000000C0000000042
00790100000030420094070000002432316432386238612D303664662D343363302D623732662D3261313631363333616
4613900000000
```

Out: uuidKey, attributes = { * }

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

```
42007B010000022042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004AFBED2C42000D0200000004000000010000000042000F01000001C842
005C0500000004000000C000000042007F0500000004000000000000000042007C01000001A042009407000000024323
16432386238612D303664662D343363302D623732662D32613136313633336164613900000000042000A07000000144372
7970746F6772617068696320 4C656E6774680000000042000A070000001743727970746F6772617068696320416C676F7
```

9

Client A:

Get attributes

In: uuidKey, attributeName = { ‘State’ }

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

```
42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000005842005C0500000004000000000B0000000042
007901000000404200940700000024323164323862386 12D303664662D343363302D623732662D32613136313633333616
46139000000000042000A070000000553746174650000000
```

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) 42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040 000000000000000420092090000000800000004AFBED2C42000D0200000004000000010000000042000F010000008042 005C0500000004000000B000000042007F0500000004000000000000000042007C0100000058420094070000002432 3 16432386238612D303664662D343363302D623732662D32613136313633336164613900000000420008010000002042000 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 420078010000016042007701000000384200690100000020420006A0200000004000000010000000042006B02000000040 000000000000000042000D0200000004000000020000000042000F010000008842005C0500000004000000D00000000042 0093080000000089D407FFB45C95672420079010000006042009407000000243231643238623861 2D303664662D3433633 02D623732662D32613136313633336164613900000000420008010000002842000A070000000C782D6174747269627574 65310000000042000B0700000006566 16C75653100042000F010000008842005C0500000004000000D000000000420093 0800000008D62107C3158409D84200790100000060420094070000002432316432386238612D303664662D343363302D 623732662D32613136313633336164613900000000420008010000002842000A070000000C782D6174747269627574653 20000000042000B070000000656616C7565320000

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

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

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

```
42007B010000019042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000000 4AFBED2C42000D0200000004000000020000000042000F010000009842
005C05000000040000000D0000000042009308000000089D407FFB45C9567242007F0500000004000000000000000000420
07C01000000604200940700000024323164323862386 12D303664662D343363302D623732662D32613136313633336164
613900000000420008010000002842000A070000000C782D617474726962757465310000000042000B070000000656616
C75653100000042000F010000009842005C05000000040000000D00000000420093080000000 8D62107C3158409D842007F
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:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 47FB42CCECA3F6EC
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-
2a161633ada9
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 08019A230A05E9E1
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-
2a161633ada9
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2
```

```
42007801000001704200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000020000000042000F010000009042005C0500000004000000E0000000042
0093080000000847FB42CCECA3F6EC4200790100000068420094070000002432316432386238612D303664662D3433633
02D623732662D326131363136333361646139000000000420008010000003042000A070000000C782D6174747269627574
65310000000042000B070000000E4D6F646966696564566616C75653100000042000F010000009042005C050000000400000
00E00000000420093080000000808019A230A05E9E14200790100000068420094070000002432316432386238612D3036
64662D343363302D623732662D326131363136333361646139000000000420008010000003042000A070000000C782D617
4747269627574653200000000042000B070000000E4D6F646966696564566616C7565320000
```

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

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

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2D (Thu Nov 12
12:10:37 CET 2009)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 47FB42CCECA3F6EC
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-
2a161633ada9
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute1
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue1
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 08019A230A05E9E1
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-
2a161633ada9
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: ModifiedValue2
```

```
42007B01000001A042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004AFBED2D42000D0200000004000000020000000042000F01000000A042
005C050000000400000000E00000000420093080000000847FB42CCECA3F6EC42007F05000000040000000000000000420
07C01000000684200940700000024323164323862386 12D303664662D343363302D623732662D3261313631363333616 4
61390000000004200080100000030 42000A070000000C782D61747472696275746531000000000 42000B070000000E4D6F6
4696669656456616C7565310000 42000F01000000A042005C050000000400000000E0000000042009308000000000808019A
230A05E9E142007F050000000400000000000000000042007C0100000068420094070000002432316432386238612D30366
4662D343363302D623732662D32613136313633336164613900000000420008010000003042000A070000000C782D6174
747269627574653200000000 42000B070000000E4D6F646966696564 56616C7565320000
```

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
```

```
42007801000001304200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000020000000042000F010000007042005C050000000400000000F0000000042
0093080000000083E2C080FA880605742007901000000484200940700000024323164323862386 12D303664662D3433633
02D623732662D3261313631363333616461390000000042000A070000000C782D617474726962757465310000000004200
0F010000007042005C050000000400000000F0000000042009308000000089D55988D43D23B82420079010000004842009
4070000002432316432386238612D303664662D343363302D623732662D32613136313633336164613900000000 42000A
070000000C782D6174747269627574653200000000
```

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

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

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

```
42007B01000001A042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000420092090000000800000000 4AFBED2D42000D0200000004000000020000000042000F01000000A042
005C05000000040000000F0000000042009308000000083E2C080FA880605742007F050000000400000000000000000420
07C0100000068420094070000002432316432386238612D303664662D343363302D623732662D32613136313633336164
613900000000420008010000003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F6
4696669656456616C756531000042000F01000000A042005C05000000040000000F0000000042009308000000089D5598
8D43D23B8242007F0500000004000000000000000042007C0100000068420094070000002432316432386238612D30366
4662D343363302D623732662D326131363136333361646139000000004200080100000030 42000A070000000C782D6174
7472696275746532000000000042000B070000000E4D6F64696669656456616C7565320000
```

13

Client A:

Get (symmetric key)

In: uuidKey

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

```
420078010000009042007701000000384200690100000020420006A020000000400000001000000004200 6B02000000040
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000 0A0000000042
007901000000304200940700000024323164323862386 12D303664662D343363302D623732662D3261313631363333616
4613900000000
```

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)
```

```
42007B010000012042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000042009209000000080000000004AFBED2D42000D0200000004000000010000000042000F01000000C842
005C0500000004000000 0A0000000042007F05000000040000000000000000042007C01000000A042005705000000004000
000020000000004200940700000024323164323862386 12D303664662D343363302D623732662D32613136313633336164
6139000000000042008F010000005842004001000000504200420500000004000000010000000042004501000000184200 4
30800000010EF7833AB15F5A1EE5874BC0D9BBC4BE742002805000000040000000300000000042002A0200000004000000
8000000000
```

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)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 21d28b8a-06df-43c0-b72f-
2a161633ada9
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000042
00790100000030420094070000002432316432386238612D303664662D343363302D623732662D32613136313633333616
4613900000000
```

Out: uuidKey

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

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000004200920900000008000000004AFBED2E42000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F0500000004000000000000000042007C01000000304200940700000024323
16432386238612D303664662D343363302D623732662D326131363136333361646139000000000
```

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 (one of them also verifying the amount that can be received using the Check operation), while a third fails since the usage allocation has been used up. The key is finally 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:

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
```

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:
    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
```

```
42007B01000000C042007A0100000048420069010000002042006A02000000040000000100000000042006B020000000400
00000000000000420092090000000080000000004AFBED2E42000D02000000040000000100000000042000F01000000684200
5C05000000040000000100000000042007F05000000040000000000000000042007C01000000404200570500000000400000000
020000000042009407000000243664326235353638 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)
```

```
42007801000001684200770100000038420069010000002042006A02000000040000000100000000042006B020000000400
000000000000000042000D0200000004000000020000000042000F01000000884200 5C050000000400000000D000000004200
9308000000833150E6CB1ACF86942007901000000604200940700000024366432623535363 82D643862342D343064312D
393930642D34626130626434666637366600000000420008010000002842000A070000000F416374697661746 96F6E2044
6174650042000B09000000080000000000000002 42000F01000000904200 5C05000000040000000D00000000 4200930800
000008CF90BC88AE42CBC24200790100000068420094070000002436643262353536382D643862342D343064312D393930
642D34626130626434666637366600000000420008010000003042000A07000000115072 6F746563742053746F70204461
```

```
746500000000000000042000B09000000008000000004AFBEF86
```

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 7A0100000048420069010000002042006A020000000400000001000000042006B020000000400
```

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)
      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)
```

```
42007801000000C84200770100000038420069010000002042006A0200000004000000010000000042006B020000000400
000000000000042000D0200000004000000010000000042000F01000000804200 5C0500000004000000D000000004200
7901000000684200940700000024366432623535363 82D643862342D343064312D393930642D3462613062643466663736
66000000004200080100000030 42000A070000000C5573616765204C696D697473000000000 42000B01000000104200980 4
00000008000000000000003E8
```

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)
```

```
42007B01000000F842007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400
000000000000042009209000000080000000004AFBED2F42000D0200000004000000010000000042000F01000000A04200
5C0500000004000000D0000000042007F0500000004000000000000000042007C01000000784200940700000024366432
62353536382D643862342D343064312D393930642D34626130626434666637366600000000420008010000004042000A07
0000000C5573616765204C696D69747300000000042000B01000000204200980400000008000000000000003E84200960400
0000080000000000000003E8
```

3

Client B:

Locate (symmetric key by name)

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

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

```
42007801000000D04200770100000038420069010000002042006A0200000004000000010000000042006B02000000400
000000000000042000D0200000004000000010000000042000F01000000884 2005C0500000004000000080000000004200
```

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
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400
00000000000000420092090000000800000004AFBED2F42000D0200000004000000010000000042000F01000000584200
5C05000000040000000800000000042007F0500000004000000000000000042007C01000000304200940700000024366432
62353536382D643862342D343064312D393930642D34626130626434666637366600000000
```

4	Client B: Get (symmetric key)

In: uuidKey

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

42007801000000904200770100000038420069010000002042006A02000000040000000100000000042006B020000000400
0000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000A000000004200
790100000030420094070000002436643262353536382D643862342D343064312D393930642D346261306264346663736
6600000000

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)
```

42007B010000012042007A0100000048420069010000002042006A02000000040000000100000000042006B020000000400
0000000000000420092090000000800000004AFBED2F42000D0200000004000000010000000042000F01000000C84200
5C0500000004000000A000000000042007F0500000004000000000000000042007C01000000A0420057050000000400000
0200000000420094070000002436643262353536382D643862342D343064312D393930642D34626130626434666373666
000000042008F010000005842004001000000504200420500000004000000010000000042004501000000184200430800
0000107C228050CE4FADBFF51227C891117F9C42002805000000040000000300000000042002A0200000004000000800000

```
0000
```

5 Client B:

Check

Get usage allocation

In (header): BatchOrderOption='true'

In: uuidKey, UsageAllocationBytes='500'

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 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: 0x00000009 (Check)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 96A635FBB610529B
    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: 00000000000001F4
(500)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3C01D168ADA81F46
    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: 00000000000001F4
(500)

42007801000001304200770100000048420069010000002042006A0200000004000000010000000042006B020000000400
0000000000000420010060000000800000000000000142000D0200000004000000020000000042000F01000000684200
5C050000000400000009000000004200930800000000896A635FBB610529B42007901000000404200940700000024366432
62353536382D643862342D343064312D393930642D3462613062643466663736660000000042009604000000080000000
000001F442000F010000006842005C0500000004000000110000000042009308000000083C01D168ADA81F464200790100
00004042009407000000243664326235353638 2D643862342D343064312D393930642D3462613062643466663736660000
00004200960400000008000000000000001F4
```

Out: uuidKey

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004AFBED2F (Thu Nov 12
12:10:39 CET 2009)
```

Deleted:

```
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)¶
¶
42007801000000A04200770100000003842006901000000020420 06A02000000004000000010000000042006B0200000000400000000000000042000D020000000040000000010000000042000F01000000058420 05C050000000040000000110000000042007901000000040420094070000002436643262353536382D643862342D343064312D393930642D34626130626434666637366600000000420096040000000080000000000001F4
```

```
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000009 (Check)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 96A635FBB610529B
    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: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 3C01D168ADA81F46
    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
```

```
42007B010000013042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400
000000000000004200920900000008000000004AFBED2F42000D0200000004000000020000000042000F01000000684200
5C0500000004000000090000000042009308000000896A635FBB610529B42007F0500000004000000000000000042007C
010000003042009407000000243664326235353638 2D643862342D343064312D393930642D3462613062643466663736 66
000000000042000F01000000 6842005C05000000040000001100000000420093080000000083C01D168ADA81F4642007F0500
00000400000000000000000042007C010000003042009407000000243664326235353638 2D643862342D343064312D393930
642D346261306264346666373666 00000000
```

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:
      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)
```

```
42007801000000A0420077010000003842006901000000 2042006A0200000004000000010000000042006B020000000400
000000000000000042000D0200000004000000010000000042000F010000005842005C050000000400000011000000004200
79010000004042009407000000243664326235353638 2D643862342D343064312D393930642D34626130626434666637 36
66000000000042009604000000080000000000001F4
```

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)
```

Deleted: ¶

```
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¶
¶
42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000004200
6B0200000004000000000000000042009209000000080000000004AFBED2F42000D020000000400000001
0000000042000F010000005842005C050000000400000011000000004200 7F05000000040000000000000000
0000 42007C010000003042009407000000243664326235353638 2D643862342D343064312D393930642D
34626130626434666637366600000000
```

```
      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
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400
000000000000004200920900000008000000004AFBED2F42000D0200000004000000010000000042000F01000000584200
5C0500000004000000110000000042007F0500000004000000000000000042007C010000003042009407000000243664 32
62353536382D643862342D343064312D393930642D34626130626434666637366600000000
```

7

Client C:

Locate (symmetric key by name)

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

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

```
42007801000000D042007701000000384200690100000020 42006A0200000004000000010000000042006B020000000400
0000000000000042000D0200000004000000010000000042000F010000008842005C0500000004000000080000000004200
79010000007042000801000000 2842000A070000000B4F626A656374205479706500000000000042000B0500000004000000
020000000042000801000000 3842000A07000000044E616D650000000042000B010000002042005507000000044B657931
000000004200540500000004000000010000000 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: 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
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400
000000000000004200920900000008000000004AFBED3042000D0200000004000000010000000042000F01000000584200
5C0500000004000000080000000042007F0500000004000000000000000042007C01000000304200940700000024366432
62353536382D643862342D343064312D393930642D346261306264346666373666600000000
```

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-
4ba0bd4ff76f
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B020000000400
000000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000000A000000004200
790100000030420094070000002436643262353536382D643862342D343064312D393930642D3462613062643466663736
6600000000
```

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)
```

```
42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400
000000000000004200920900000008000000004AFBED3042000D02000000040000000100000000042000F01000000C84200
5C050000000400000000A000000000042007F050000000400000000000000000042007C01000000A04200570500000000400000
0200000000420094070000002436643262353536382D643862342D343064312D393930642D3462613062643466666373666
000000000042008F010000005842004001000000504200420500000000400000001000000004200450100000018420043080
00000107C228050CE4FADBFF51227C891117F9C420028050000000400000003000000000042002A02000000004000000800000
0000
```

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)
  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)
```

```
42007801000000A0420077010000003842006901000000002042006A02000000040000000100000000042006B020000000400
000000000000000042000D02000000000400000001000000000042000F01000000058420005C0500000000400000011000000004200
790100000004042009407000000243664326235353638 2D643862342D343064312D393930642D346261306264346666373 6
66000000000420096040000000080000000000001F4
```

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
```

```
42007B01000000B842007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400
000000000000004200920900000008000000004AFBED3142000D0200000004000000010000000042000F01000000604200
5C05000000040000001100000000420007F05000000040000000100000000042007E05000000040000000C0000000042007D
0700000023556E61626C6520746F20616C6C6F636174652072657175657374656420616D6F756E740000000000
```

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
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042006B020000000400
00000000000000042000D02000000040000000100000000042000F01000000484200 5C050000000400000014000000004200
79010000003042009407000000243664326235353638 2D643862342D343064312D393930642D346261306264346666373736
6600000000
```

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
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042006B020000000400
000000000000004200920900000008000000004AFBED3142000D0200000004000000010000000042000F01000000584200
5C0500000004000000140000000042007F0500000004000000000000000042007C010000003042009407000000024366432
```

```
62353536382D643862342D343064312D393930642D34626130626434666637366600000000
```

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:
    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)

42007801000001104200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
0000000000000042000D02000000040000000100000000042000F01000000C842005C05000000040000000300000000042
007901000000B04200570500000004000000020000000042009101000000384200080100000030420000A0700000018437
27970746F677261706869632055736167652204D61736B42000B020000000400000004000000000042008F01000000584200
40010000005042004205000000040000000100000000420045010000001842004308000000100123456789ABCDEF01234
56789ABCDEF4200280500000004000000030000000042002A020000000400000080000000000
```

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
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000000 4AFBED3242000D0200000004000000010000000042000F010000005842
005C0500000004000000030000000042007F0500000004000000000000000042007C010000003042009407000000024366
53161356138332D383131332D343236302D623430642D39363666323331623931623700000000
```

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:
      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
```

```
42007801000000C0420077010000003842006901000000200042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F010000007842005C05000000040000000D0000000042
007901000000604200940700000024366531613561383332D383131332D343236302D623430642D39363666323331623933
1623700000000420008010000002842000A070000000A782D70726F766964657200000000000042000B0700000007756E
6B6E6F776E00
```

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

42007B01000000E042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004AFBED3242000D0200000004000000010000000042000F010000008842
005C0500000004000000D0000000042007F0500000004000000000000000042007C0100000006042009407000000024366
53161356138332D383131332D343236302D623430642D39363666323331623931623700000000420008010000000284200
0A070000000A782D70726F76696465720000000000000042000B0700000007756E6B6E6F776E00
```

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)
    Tag: 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

42007801000000C84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000008042005C0500000004000000E0000000042
0079010000006842009407000000243665316135613833322D383131332D343236302D623430642D39363666323331623931
6237000000000420008010000003042000A070000000A782D70726F7669646572000000000000042000B070000000B7468
6972642070617274790000000000
```

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
```

```
42007B01000000E842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000000 4AFBED3242000D02000000040000000100000000042000F0100000090 42
005C050000000400000000E000000042007F0500000004000000000000000042007C0100000068420094070000002436 6
5316135613833 32D383131332D343236302D623430642D3936366632333162393162370000000042000801000000304200
0A070000000A782D70726F766964657200000000000042000B070000000B7468697264207061727479000000000000
```

3

Destroy (symmetric key)

In: uuidKey

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

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000140000000042
00790100000030420094070000002436653161356138332D383131332D343236302D623430642D3936366632333162393
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


42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420006B02000000040
000000000000000420092090000000080000000004AFBED3242000D0200000004000000010000000042000F010000005842
005C05000000004000000140000000042007F050000000040000000000000000042007C0100000030420094070000002436
6531613561383332D383131332D343236302D623430642D39363666323331623931623700000000
```

7 Vendor Extensions

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

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

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

Time	Client A
0	Create (symmetric key) In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C' }, MessageExtension={ VendorIdentification='Acme', CriticalityIndicator='false', VendorExtension={ tag='0x540001', type='text string', value='na' } }

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

Formatted: Font: Courier New, 8 pt, Font color: Black

```
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)
    Tag: Message Extension (0x420051), Type: Structure (0x01), Data:
      Tag: Criticality Indicator (0x420026), Type: Boolean (0x06), Data: FALSE
      Tag: Vendor Identification (0x42009D), Type: Text String (0x07), Data: Acme
      Tag: Vendor Extension (0x42009C), Type: Structure (0x01), Data:
        Tag: Unknown tag (0x014242), Type: Text String (0x07), Data: na

42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F01000001184200 5C0500000004000000010000000042
007901000000C04200570500000004000000020000000042009101000000A84200080100000030 42000A070000001443 7
27970746F6772617068696320 4C656E6774680000000042000B020000000400000080000000004200080100000030 4200
0A07000000174372797074 6F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000
80100000030 42000A070000001843727970746F677261706869632055736167652 04D61736B42000B02000000040000000
0C00000000420051010000003842002606000000080000000000000000 42009D070000000441636D650000000042009C0
10000001001424207000000026E61000000000000
```

Out: objectType='00000002', uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73BF1C (Thu Feb 11 09:26:04 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 052eff73-b35e-4702-9db9-37c12f0151d3

42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B73BF1C42000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F0500000004000000000000000042007C01000000404200570500000004000
0000200000000420094070000002430353265666637332D623335652D343730322D396462392D3337633132663031353 1
643300000000
```

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:
```

Formatted: Font: Courier New, 8 pt, Font color: Black

Formatted: Font: Courier New, 8 pt, Font color: Black

```
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 052eff73-b35e-4702-9db9-
37c12f0151d3

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000042
00790100000030420094070000002430353265666637332D623335652D343730322D396462392D33376331326630313 53
1643300000000
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73BF1C (Thu Feb 11
09:26:04 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 052eff73-b35e-4702-9db9-
37c12f0151d3

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B73BF1C42000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F050000000400000000000000000042007C010000003042009407000000024303
53265666637332D623335652D343730322D396462392D3337633132663031353164330000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

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' } }

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

Formatted: Font: Courier New, 8 pt, Font color: Black

```
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt,
Decrypt)
    Tag: Message Extension (0x420051), Type: Structure (0x01), Data:
      Tag: Criticality Indicator (0x420026), Type: Boolean (0x06), Data: TRUE
      Tag: Vendor Identification (0x42009D), Type: Text String (0x07), Data: Acme
      Tag: Vendor Extension (0x42009C), Type: Structure (0x01), Data:
        Tag: Unknown tag (0x014242), Type: Text String (0x07), Data: na
```

```
42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000011842005C0500000004000000010000000042
007901000000C04200570500000004000000020000000042009101000000A84200080100000030420000A0700000014437
27970746F67726170686963204C656E67746800000000042000B02000000040000008000000000420008010000000304200
0A07000000174372797074F6772617068696320416C676F726974686D0042000B050000000400000003000000042000
801000000030420000A07000000184372797074F6772617068696320557361676520AD61736B42000B0200000004000000
0C000000004200510100000038420026060000000800000000000000142009D070000000441636D650000000042009C0
1000000100142420700000026E61000000000000
```

Out: Operation Failed, Feature Not Supported

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73BF1D (Thu Feb 11
09:26:05 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)
    Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x00000008 (Feature Not
Supported)
    Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Critical Message Extension
not recognized
```

Formatted: Font: Courier New, 8 pt, Font color: Black

<table>
<tr><td></td><td>42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000000800000000 4B73BF1D42000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F0500000004000000010000000042007E05000000040000000800000000420
07D0700000029437269746963616C204D657373616765204578746656E73696F6E206E6F74207265636F676E697A656400
000000000000</td></tr>
</table>

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.

<table>
<tr><th>Time</th><th>Client A</th></tr>
<tr><td>0</td><td>Create Key Pair

In: commonAttributes={ CryptographicAlgorithm='RSA', CryptographicLength='1024' }, privateKeyAttributes={ Name={ NameValue='PrivateKey1', NameType='00000001' }, CryptographicUsageMask='00000001' }, publicKeyAttributes={ NameValue='PublicKey1', NameType='00000001' }, CryptographicUsageMask='00000002' }
<pre>
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000002 (Create Key Pair)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Common Template-Attribute (0x42001F), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (RSA)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000400 (1024)
      Tag: Private Key Template-Attribute (0x420065), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: PrivateKey1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
</pre></td></tr>
</table>

Deleted: , CryptographicUsageMask='0000000C'

Formatted: Font: Courier New, 8 pt, Font color: Black

```
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000001 (Sign)
      Tag: Public Key Template-Attribute (0x42006E), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: PublicKey1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000002 (Verify)
```

```
42007801000001E84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000001A042005C0500000004000000020000000042
0079010000018842001F0100000070420008010000003042000A07000000174372797074672617068696320416C676
```

Out: uuidPrivateKey, uuidPublicKey

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

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007B01000000E042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B73C13A42000D0200000004000000010000000042000F010000008842
005C0500000004000000020000000042007F0500000004000000000000000042007C01000000604200940700000024383
935663732633322D623230612D343964382D393530342D366463323131356363303432000000004200940700000246132
3432666361342D656266302D343339382D616336352D38373962616234393032353900000000
```

Formatted: Font: 8 pt, Font color: Black

1 Locate (Public Key)

In: attributes={ objectType='PublicKey', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (Public Key)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000103 (Private Key
Link)
          Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: a242fca4-
ebf0-4398-ac65-879bab490259
```

```
42007801000000F042007701000000384200690100000020420006A02000000040000000100000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F01000000A842005C0500000004000000080000000042
007901000000904200080100000028420000A070000000B4F626A65637420547970650000000000042000B0500000004000
00003000000004200080100000058420000A07000000044C696E6B0000000042000B01000000404200 4B05000000040000
0103000000000042004C07000000246132343266636134 2D656266302D343339382D616336352D383739626162343930323
53900000000
```

Out: uuidPublicKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13B (Thu Feb 11
09:35:07 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-
6dc2115cc042
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004B73C13B42000D0200000004000000010000000042000F01000000005842
005C050000000400000008000000000042007F0500000004000000000000000042007C0100000003042009407000000024383
935663732633222D623230612D343964382D393530342D366463323131356363303432000000000
```

2	Locate (Private Key)

Formatted: Font: Courier New, 8 pt, Font color: Black

Formatted: Font: Courier New, 8 pt, Font color: Black

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

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Private Key)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000102 (Public Key Link)
          Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: 895f72c2-
b20a-49d8-9504-6dc2115cc042
```

Formatted: Font: Courier New, 8 pt, Font color: Black

42007801000000F04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000000A842005C050000000400000008000000000042
00790100000090420008010000002842000A070000000B4F626A65637420547970650000000000042000B0500000004000
000040000000004200080100000005842000A070000000044C696E6B0000000042000B010000004042004B050000000400000
010200000000042004C0700000024383935663732633322D623230612D343964382D393530342D366463323131356363303
43200000000

Out: uuidPrivateKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13B (Thu Feb 11
09:35:07 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-
879bab490259
```

Formatted: Font: Courier New, 8 pt, Font color: Black

42007B01000000B042007A01000000484200690100000020420006A0200000004000000010000000042006B02000000040
000000000000000042009209000000080000000004B73C13B42000D0200000004000000010000000042000F010000005842
005C0500000004000000080000000042007F0500000004000000000000000042007C010000003042009407000000024613
23432666361342D656266302D343339382D616336352D38373962616234393032353900000000

3	Destroy

In: uuidPrivateKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-
879bab490259
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000420006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000000042
0079010000003042009407000000246132343266636134 2D656266302D343339382D616336352D38373962616234393 03
2353900000000
```

Out: uuidPrivateKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13B (Thu Feb 11
09:35:07 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a242fca4-ebf0-4398-ac65-
879bab490259
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042009209000000080000000004B73C13B42000D0200000004000000010000000042000F010000005842
005C050000000400000014000000000042007F0500000004000000000000000042007C010000003042009407000000024613
23432666361342D656266302D343339382D616336352D383739626162343930323539000000000
```

4

Destroy

In: uuidPublicKey

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

Formatted: Font: Courier New, 8 pt, Font color: Black

```
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-6dc2115cc042

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000001400000000042
0079010000003042009407000000243839356637326332 2D623230612D343964382D393530342D3664633231313563633
0343200000000
```

Out: uuidPublicKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C13B (Thu Feb 11 09:35:07 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 895f72c2-b20a-49d8-9504-6dc2115cc042

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000004200920900000008000000004B73C13B42000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002438393
5663732633222D623230612D343964382D393530342D3664633231313563633034320000000000
```

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='00000001' }, foreignPrivateKey

```
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)
```

Formatted: Font: Courier New, 8 pt, Font color: Black

Deleted: C

Formatted: Font: Courier New, 8 pt, Font color: Black

```
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000004 (Private Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000001 (Sign)
      Tag: Private Key (0x420064), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000004
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data:
30820276020100300D06092A864886F70D0101010500048202603082025C02010002818100930451C9ECD94F5BB9DA17D
D09381BD23BE43ECA8C7539F301FC8A8CD5D5274C3E7699DBDC711C97A7AA91E2C50A82BD0B1034F0DF493DEC16362427
E58ACCE7F6CE0F9BCC617BBD8C90D0094A2703BA0D09EB19D1005F2FB265526AAC75AF32F8BC782CDED2A57F811E03EAF
67A944DE5E78413DCA8F232D074E6DCEA4CEC9F02030100010281800B6A7D736199EA48A420E4537CA0C7C046784DCBEA
A63BAEBC0BC132787449CDE8D7CAD0C0C863C0FEFB06C3062BEFC50033ECF87B4E33A9BE7BCBC8F1511AE215E80DEB5D8
AF2BD31319D7821196640935A0CD67C94599579F2100D65E038831FDAFB0DBE2BBDAC00A696E67E756350E1C99ACE11A3
6DABAC3ED3E730960059024100DDF672FBCC5BDA3D73AFFC4E791E0C03390224405D69CCAABC749FAA0DCD4C2583C71DD
E8941A7B9AA030F52EF1451466C074D4D338FE677892ACD9E10FD35BD024100A98FBC3ED6B4C6F860F97165AC2F7BB6F2
E2CB192A9ABD49795BE5BCF37D8EE69A6E169C24E5C32E4E7FA33265461407F952BA49E204818A2F785F113F922B8B024
0253F9470390D39049303777DDBC9750E9D64849CE0903EAE704DC9F589B7680DEB9D609FD5BCD4DECD6F120542E5CFF5
D76F2A43C8615FB5B3A9213463797AA9024100A1DDF023C0CD94C019BB26D09B9E3CA8FA971CB16AA58B9BAF79D6081A1
DBBA452BA53653E2804BA98FF69E8BB1B3A161EA225EA501463216A8DAB9B88A75E5F02406178646E112CF79D921A8A84
3F17F6E7FF974F688122365BF6690CDFC996E1890952EB3820DD1890EC1C8619E87A2BD38F9D03B37FAC742EFB748C788
5942C39
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000004
(RSA)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000400 (1024)

42007801000003804200770100000038420069010000002042006A020000000400000001000000004200 6B02000000040
000000000000000042000D0200000004000000010000000042000F010000003842005C050000000400000003000000042
007901000003204200570500000004000000040000000042009101000000384200080100000030 42000A0700000018437
27970746F677261706869632055736167652 04D61736B42000B02000000040000000100000000 42006401000002C84200
4001000002C04200420500000004000000040000000042004501000002884200430800000027A30820276020100300D060
92A864886F70D0101010500048202603082025C02010002818100930451C9ECD94F5BB9DA17DD09381BD23BE43ECA8C75
39F301FC8A8CD5D5274C3E7699DBDC711C97A7AA91E2C50A82BD0B1034F0DF493DEC16362427E58ACCE7F6CE0F9BCC617
BBD8C90D0094A2703BA0D09EB19D1005F2FB265526AAC75AF32F8BC782CDED2A57F811E03EAF67A944DE5E78413DCA8F2
32D074E6DCEA4CEC9F02030100010281800B6A7D736199EA48A420E4537CA0C7C046784DCBEAA63BAEBC0BC132787449C
DE8D7CAD0C0C863C0FEFB06C3062BEFC50033ECF87B4E33A9BE7BCBC8F1511AE215E80DEB5D8AF2BD31319D7821196640
935A0CD67C94599579F2100D65E038831FDAFB0DBE2BBDAC00A696E67E756350E1C99ACE11A36DABAC3ED3E7309600590
24100DDF672FBCC5BDA3D73AFFC4E791E0C03390224405D69CCAABC749FAA0DCD4C2583C71DDE8941A7B9AA030F52EF14
51466C074D4D338FE677892ACD9E10FD35BD024100A98FBC3ED6B4C6F860F97165AC2F7BB6F2E2CB192A9ABD49795BE5B
CF37D8EE69A6E169C24E5C32E4E7FA33265461407F952BA49E204818A2F785F113F922B8B0240253F9470390D39049303
777DDBC9750E9D64849CE0903EAE704DC9F589B7680DEB9D609FD5BCD4DECD6F120542E5CFF5D76F2A43C8615FB5B3A92
13463797AA9024100A1DDF023C0CD94C019BB26D09B9E3CA8FA971CB16AA58B9BAF79D6081A1DBBA452BA53653E2804BA
98FF69E8BB1B3A161EA225EA501463216A8DAB9B88A75E5F02406178646E112CF79D921A8A843F17F6E7FF974F6881223
65BF6690CDFC996E1890952EB3820DD1890EC1C8619E87A2BD38F9D03B37FAC742EFB748C7885942C3900000000000042
00280500000004000000040000000042002A02000000040000040000000000
```

Out: uuidPrivateKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A1 (Thu Feb 11
09:49:37 CET 2010)
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-
d66d27b11943

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000000004B73C4A142000D0200000004000000010000000042000F010000005842
005C0500000004000000030000000042007F0500000004000000000000000042007C01000000304200940700000024666
130363036386332D366662312D343265612D623661322D643636643237623131393433000000000
```

1 Register (Public Key)

In: objectType='00000004', attributes={ CryptographicUsageMask='00000002', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } }, foreignPublicKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000003 (Public Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000002 (Verify)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000103 (Private Key
Link)
            Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: fa06068c-
6fb1-42ea-b6a2-d66d27b11943
      Tag: Public Key (0x42006D), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000005
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data:
30819F300D06092A864886F70D010101050003818D0030818902818100930451C9ECD94F5BB9DA17DD09381BD23BE43EC
A8C7539F301FC8A8CD5D5274C3E7699DBDC711C97A7AA91E2C50A82BD0B1034F0DF493DEC16362427E58ACCE7F6CE0F9B
CC617BBD8C90D0094A2703BA0D09EB19D1005F2FB265526AAC75AF32F8BC782CDED2A57F811E03EAF67A944DE5E78413D
CA8F232D074E6DCEA4CEC9F0203010001
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000004
(RSA)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000400 (1024)

42007801000002084200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000001C042005C0500000004000000030000000042
```

Deleted: C

Formatted: Font: Courier New, 8 pt, Font color: Black

```
007901000001A84200570500000004000000030000000042009101000000984200080100000030420000A0700000018437
27970746F677261706869632055736167652004D61736B42000B0200000004000000020000000042000801000000584200
0A07000000044C696E6B000000042000B010000004042004B0500000004000001030000000042004C070000002466613
036303638632D366662312D343265612D623661322D643636643237623131393433000000042006D01000000F0420040
01000000E8420042050000000400000005000000004200450100000B042004308000000A230819F300D06092A864886F
70D010101050003818D0030818902818100930451C9ECD94F5BB9DA17DD09381BD23BE43ECA8C7539F301FC8A8CD5D527
4C3E7699DBDC711C97A7AA91E2C50A82BD0B1034F0DF493DEC16362427E58ACCE7F6CE0F9BCC617BBD8C90D0094A2703B
A0D09EB19D1005F2FB265526AAC75AF32F8BC782CDED2A57F811E03EAF67A944DE5E78413DCA8F232D074E6DCEA4CEC9F
02030100010000000000004200280500000004000000040000000042002A02000000040000040000000000
```

Out: uuidPublicKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A2 (Thu Feb 11
09:49:38 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 79cbf228-16df-4fb1-a385-
443546935e74
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000040
00000000000000042009209000000080000000004B73C4A242000D02000000040000000100000000042000F010000005842
005C050000000400000003000000042007F0500000004000000000000000042007C010000003042009407000000024373
96362663232382D313664662D346662312D613338352D34343335343639333565373400000000
```

2 Add attribute

In: uuidPrivateKey, attribute={ Link={ LinkType=‘PublicKeyLink’, LinkedObjectIdentifier=uuidPublicKey } }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-
d66d27b11943
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000102 (Public Key Link)
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
        Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: 79cbf228-16df-4fb1-a385-443546935e74
```

```
42007801000000F042007701000000384200690100000020420006A020000000400000001000000004200
6B020000000400000000000000000042000D0200000004000000010000000042000F01000000A842005C0
500000004000000D00000000420079010000009042009407000000246661303630363832D36666231
2D343265612D623661322D6436366432376231313934330000000042000801000000584200A0700000
0044C696E6B0000000042000B01000000404200 4B050000000400000102000000000042004C070000002
437396362663232382D313664662D346662312D613338352D34343335343639333565373400000000
```

Out: uuidPrivateKey, attribute={ Link={ LinkType=‘PublicKeyLink’, LinkedObjectIdentifier=uuidPublicKey } }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A2 (Thu Feb 11
09:49:38 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-
d66d27b11943
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000102 (Public Key Link)
          Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: 79cbf228-
16df-4fb1-a385-443546935e74
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007B010000011042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004B73C4A242000D0200000004000000010000000042000F01000000B842
005C050000000400000000D000000000042007F050000000400000000000000000042007C0100000090420094070000024666
130363036386 32D36666231 2D343265612D623661322D6436366432376231313934330000000042000801000000584200
0A07000000044C696E6B0000000042000B01000000404200 4B0500000004000001020000000042004C070000002437396
362663232382D313664662D346662312D613338352D34343335343639333565373400000000
```

3 Locate (Public Key)

In: attributes={ objectType=’PublicKey’, Link={ LinkType=‘PrivateKeyLink’, LinkedObjectIdentifier=uuidPrivateKey } }

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

Formatted: Font: Courier New, 8 pt, Font color: Black

```
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (Public Key)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000103 (Private Key
Link)
          Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: fa06068c-
6fb1-42ea-b6a2-d66d27b11943
```

```
42007801000000F04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000000A842005C0500000004000000080000000042
00790100000090420008010000002842000A070000000B4F626A65637420547970650000000000042000B0500000004000
000030000000042000801000000058420000A07000000044C696E6B0000000042000B010000004042004B05000000040000
010300000000042004C07000000024666130363036386632D366662312D343265612D623661322D6436366643237623131393
43300000000
```

Out: uuidPublicKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A2 (Thu Feb 11
09:49:38 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 79cbf228-16df-4fb1-a385-
443546935e74
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B73C4A242000D0200000004000000010000000042000F010000005842
005C0500000004000000080000000042007F050000000400000000000000042007C0100000030420094070000000024373
96362663232382D313664662D346662312D613338352D343433353436393335653734000000000
```

4 Locate (Private Key)

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

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

Formatted: Font: Courier New, 8 pt, Font color: Black

Formatted: Font: Courier New, 8 pt, Font color: Black

```
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Private Key)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000102 (Public Key Link)
          Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: 79cbf228-
16df-4fb1-a385-443546935e74
```

```
42007801000000F04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000000A842005C050000000400000008000000042
00790100000090420008010000002842000A070000000B4F626A656374205479706500000000000042000B0500000004000
0000400000000420008010000005842000A07000000044C696E6B0000000042000B01000000404200 4B05000000040000
01020000000042004C0700000024373963626632382D313664662D346662312D613338352D3434333534363933356 53
73400000000
```

Out: uuidPrivateKey

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

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000004200920900000008000000004B73C4A342000D0200000004000000010000000042000F010000005842
005C0500000004000000080000000042007F0500000004000000000000000042007C0100000030420094070000002466 66
130363036386 32D366662312D343265612D623661322D643636643237623131393433 00000000
```

5 Destroy

In: uuidPrivateKey

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

Formatted: Font: Courier New, 8 pt, Font color: Black

	Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66d27b11943 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040 000000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000140000000042 0079010000003042009407000000246661303630363863 2D366662312D343265612D623661322D6436366432376231313 9343300000000 Out: uuidPrivateKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A3 (Thu Feb 11 09:49:39 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fa06068c-6fb1-42ea-b6a2-d66d27b11943 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040 00000000000000004200920900000008000000004B73C4A342000D0200000004000000010000000042000F010000005842 005C0500000004000000140000000042007F0500000004000000000000000042007C010000003042009407000000024666 13036303638632D366662312D343265612D623661322D643636643237623131393433300000000
6	Destroy In: uuidPublicKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 79cbf228-16df-4fb1-a385-443546935e74 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040 000000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000140000000042 0079010000003042009407000000243739636266323238 2D313664662D346662312D613338352D3434333534363933356 5373400000000

Formatted: Font: Courier New, 8 pt, Font color: Black

Formatted: Font: Courier New, 8 pt, Font color: Black

	Out: uuidPublicKey
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C4A3 (Thu Feb 11 09:49:39 CET 2010)
	    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
	    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 79cbf228-16df-4fb1-a385-443546935e74
	
	42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
	0000000000000004200920900000008000000004B73C4A342000D0200000004000000010000000042000F010000005842
	005C050000000400000014000000004 2007F0500000004000000000000000042007C0100000030420094070000002437 3
	96362663232382D313664662D346662312D613338352D34343335343639333565373400000000

Formatted: Font: Courier New, 8 pt, Font color: Black

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' } }
	
	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:

Formatted: Font: Courier New, 8 pt, Font color: Black

```
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt,
Decrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
```

```
420078010000016042007701000000384200690100000020420 06A02000000040000000100000000420 06B02000000040
```

Out: objectType='00000002', uuidKey

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

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B73C8BA42000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F0500000004000000000000000042007C010000004042005705000000004000
0000200000000420094070000002466623536303733352D656636662D343038352D396530612D6562366631333934633 2
```

Formatted: Font: 8 pt, Font color: Black

```
313800000000
```

1 Locate

In: attributes={ Name={ NameValue=‘rekeyKey’, NameType=’00000001’ } }

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

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042
0079010000004042000801000000384200A07000000044E616D650000000042000B010000002042005507000000008726
56B65794B65794200540500000004000000010000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BA (Thu Feb 11
10:07:06 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-
eb6f1394c218

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004B73C8BA42000D0200000004000000010000000042000F010000005842
005C0500000004000000080000000042007F0500000004000000000000000042007C010000003042009407000000024666
23536303733352D656636662D343038352D396530612D65623666313339346332313800000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

2 Rekey

In: uuidKey

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

Formatted: Font: Courier New, 8 pt, Font color: Black

```
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-
eb6f1394c218

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000040000000042
0079010000003042009407000000246662353630373352D656636662D343038352D396530612D6562366631333934633
2313800000000
```

Out: uuidNewKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BB (Thu Feb 11
10:07:07 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: bf6cc1d4-f914-4099-b4d4-
453050d8bcf4

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004B73C8BB42000D0200000004000000010000000042000F010000005842
005C0500000004000000040000000042007F0500000004000000000000000042007C010000003042009407000000024626
63663633164342D663931342D343039392D623464342D34353330353064386263663400000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

3 Locate

In: attributes={ Name={ NameValue=‘rekeyKey’, NameType=’00000001’ } }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
```

Formatted: Font: Courier New, 8 pt, Font color: Black

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

42007801000000A042007701000000384200690100000020042006A02000000040000000100000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F01000000584200 5C0500000004000000080000000042
0079010000004042000801000000384200 0A07000000044E616D650000000042000B01000000204200550700000008726
56B65794B6579420054050000000400000001000000000
```

Out: uuidNewKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BB (Thu Feb 11
10:07:07 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: bf6cc1d4-f914-4099-b4d4-
453050d8bcf4

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000420092090000000800000004B73C8BB42000D0200000004000000010000000042000F010000005842
005C050000000400000008000000042007F050000000400000000000000042007C010000003042009407000000024626
63663633164342D663931342D343039392D623464342D34353330353064386263663400000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

4 Get Attribute

In: uuidKey, attributeName={‘Name’}

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

42007801000000A042007701000000384200690100000002042006A02000000040000000100000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F01000000584200 5C05000000040000000B0000000042
00790100000040420094070000002466623536303733352D656636662D343038352D396530612D656236663133393463
32313800000000042000A07000000044E616D6500000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

Out: uuidKey

Deleted: 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: 0x000000004B73C8BB (Thu Feb 11
10:07:07 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-
eb6f1394c218
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007B01000000B042007A01000000484200690100000020420 06A0200000004000000010000000042006B02000000040
000000000000000420092090000000080000000004B73C8BB42000D0200000004000000010000000042000F010000005842
005C05000000040000000B0000000042007F0500000004000000000000000042007C0100000030420094070000002466 6
23536303733352D656636662D343038352D396530612D65623666313339346332313800000000
```

5 Get (symmetric key)

In: uuidKey

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

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000000A0000000042
007901000000304200940700000024666235363037333 52D656636662D343038352D396530612D65623666313339346 33
2313800000000
```

Out: objectType = ‘00000002’, uuidKey, symmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BB (Thu Feb 11
```

Formatted: Font: Courier New, 8 pt, Font color: Black

Formatted: Font: Courier New, 8 pt, Font color: Black

```
10:07:07 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-
eb6f1394c218
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data:
BC25617991C49D06536008D076017462
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003
(AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)

42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000080000004B73C8BB42000D0200000004000000010000000042000F01000000C842
005C0500000004000000A0000000042007F0500000004000000000000000042007C01000000A0420057050000000004000
0000200000000420094070000002466623536303733352D656636662D343038352D396530612D6562366631333934633 2
313800000000042008F010000005842004001000000504200420500000004000000010000000042004501000000184200 4
30800000010BC25617991C49D06536008D07601746242002805000000040000000300000000420 02A020000000400000 0
8000000000
```

6 Destroy

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-
eb6f1394c218

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F01000000484 2005C0500000004000000140000000042
007901000000304200940700000024666235363037333 52D656636662D343038352D396530612D6562366631333934633
2313800000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

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)
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73C8BC (Thu Feb 11
10:07:08 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fb560735-ef6f-4085-9e0a-
eb6f1394c218

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000004200920900000008000000004B73C8BC42000D0200000004000000010000000042000F010000005842
005C05000000040000001400000000042007F05000000040000000000000000042007C01000000304200940700000024666
23536303733352D656636662D343038352D396530612D65623666313339346332313800000000
```

7

Destroy

In: uuidNewKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: bf6cc1d4-f914-4099-b4d4-
453050d8bcf4

4200780100000090420077010000003842006901000000204200 6A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000140000000042
00790100000030420094070000002462663663633164342D663931342D343039392D623464342D3435333035306438626
3663400000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

Out: uuidNewKey

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

Formatted: Font: Courier New, 8 pt, Font color: Black

	42007B01000000B042007A01000000484200690100000020420 06A02000000040000000100000000420006B02000000040 0000000000000000420092090000000080000000004B73C8BC42000D02000000040000000100000000042000F010000005842 005C0500000000400000014000000000042007F050000000040000000000000000042007C010000003042009407000000024626 63663633164342D663931342D343039392D623464342D34353330353064386263663400000000

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

Create a new symmetric key. 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 “Deactivated”. 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.

Deleted: with a name

Deleted: e

Time	Client A

0	Create (symmetric key)
	In: objectType=’00000002’, 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: Attribute (0x420008), Type: Structure (0x01), Data:
	          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
	          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
	        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
	          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
	        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
	          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt, Decrypt)
	        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
	          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:

Formatted: Font: Courier New, 8 pt, Font color: Black

```
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
```

```
42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000011842005C0500000004000000010000000042
007901000001004200570500000004000000020000000042009101000000E842000801000000304200A0700000017437
27970746F677261706869632041 6C676F726974686D0042000B050000000400000003000000004200080100000030420 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: 0x000000004B73FFC7 (Thu Feb 11
14:01:59 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-
0575a41d93b6
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B73FFC742000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F0500000004000000000000000042007C010000004042005705000000040000
00020000000042009407000000246662633566336535 2D343862662D343239342D623735342D30353735613431643933
623600000000
```

1 Add Activation Date, Deactivation Date attributes based on Timestamp in previous response (batch)

In: uuidKey, attribute={ ActivationDate=' <*Timestamp in previous response – 365 days*>' }

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

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BAC4A9CECC650259
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
0575a41d93b6
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004992CC47 (Wed
Feb 11 14:01:59 CET 2009)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 582C952324F4552F
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-
0575a41d93b6
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B74003F (Thu
Feb 11 14:03:59 CET 2010)
```

```
42007801000001784200770100000048420069010000002042006A02000000040000000100000000042006B02000000040
00000000000000004200100600000000800000000000000001420000D0200000004000000020000000042000F010000008842
005C05000000040000000D00000000420093080000008BAC4A9CECC650259420079010000006042009407000000024666
263356633365352D343862662D343239342D623735342D303537356134316439336236000000004200080100000028420
0A070000000F41637469766174696F6E2044617465042000B09000000080000000004992CC4742000F010000009042005
C05000000040000000D00000000420093080000008582C952324F4552F420079010000006842009407000000024666263
35663365352D343862662D343239342D623735342D30353735613431643933623600000000420008010000003042000A0
70000001144656163746976617469696F6E2044617465000000000000000042000B09000000080000000004B74003F
```

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

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

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73FFC7 (Thu Feb 11
14:01:59 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BAC4A9CECC650259
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-
0575a41d93b6
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004992CC47 (Wed
Feb 11 14:01:59 CET 2009)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 582C952324F4552F
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
0575a41d93b6
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B74003F (Thu
Feb 11 14:03:59 CET 2010)
```

42007B010000019842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004B73FFC742000D0200000004000000020000000042000F010000009842
005C0500000004000000D0000000042009308000000008BAC4A9CECC65025942007F0500000004000000000000000420
07C0100000060420094070000002466626335663365352D343862662D343239342D623735342D303537356134316439 33
62360000000042000801000000284200A070000000F416374697661746F6E20446174650042000B090000000800000
0004992CC4742000F01000000A042005C0500000004000000D000000004200930800000008582C952324F4552F42007F
05000000040000000000000000042007C0100000068420094070000002466626335663365352D343862662D343239342D6
23735342D3035373561343164393362360000000042000801000000304200A0700000011446561637469766174696F6E
20446174650000000000000042000B09000000080000000004B74003F

2

Get Attribute * *Repeated until state changes to Deactivated*

In: uuidKey, attributeName={'State'}

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-
0575a41d93b6
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
```

Formatted: Font: Courier New, 8 pt, Font color: Black

42007801000000A0420077010000003842006901000000204200 6A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000005842005C05000000040000000B0000000042
00790100000040420094070000002466626335663365352D343862662D343239342D623735342D30353735613431643 93
36236000000000042000A070000000553746174650000000

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

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B73FFC7 (Thu Feb 11
14:01:59 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-
0575a41d93b6
```

Formatted: Font: Courier New, 8 pt, Font color: Black

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

42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B73FFC742000D0200000004000000010000000042000F010000008042
005C0500000004000000B0000000042007F0500000004000000000000000042007C0100000058420094070000000024666
26335663365352D343862662D343239342D623735342D30353735613431643933623600000000420008010000002004200
0A070000000553746174650000000042000B05000000040000000200000000
```

3 Get Attribute

In: uuidKey, attributeName={‘State’}

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-
0575a41d93b6
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

420078010000000A042007701000000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000000058420005C0500000004000000B0000000042
0079010000000404200940700000002466626335663365352D343862662D343239342D623735342D3035373561343164393
36236000000000042000A070000000553746174650000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

Out: uuidKey, attribute={ State=‘*Deactivated*’ }

Deleted: *e*

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

42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
000000000000000042009209000000080000000004B74004042000D02000000040000000100000000042000F010000008042
005C05000000040000000B000000000042007F0500000004000000000000000042007C010000005842009407000000024666
26335663365352D343862662D343239342D623735342D30353735613431643933623600000000420008010000002042000
0A07000000005537461746500000042000B0500000004000000030000000000
```

4

Rekey

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

Deleted: 018B8200

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

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007801000000A042007701000000384200690100000020042006A02000000040000000100000000042006B02000000040
000000000000000042000D02000000040000000100000000042000F010000005842005C050000000400000004000000000042
007901000000404200940700000024666263356633365352D343862662D343239342D623735342D303537356134316439 3
3623600000000004200580A00000004FE747E0000000000
```

Out: uuidNewKey

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

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007B01000000B042007A01000000484200690100000020042006A02000000040000000100000000042006B02000000040
000000000000000042009209000000080000000004B74004042000D02000000040000000100000000042000F010000005842
005C05000000040000000400000000042007F0500000004000000000000000042007C010000003042009407000000024333
83936303262312D636130322D346333632D623561332D6333373839653766326339320000000
```

5

Get Attribute

In: uuidNewKey, attributeName={' ActivationDate', 'DectivationDate' }

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

Formatted: Font: Courier New, 8 pt, Font color: Black

```
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-
c3789e7f2c92
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date
```

```
42007801000000C84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000008042005C0500000004000000000B0000000042
007901000000684200940700000024333839363032623132D636130322D346333632D623561332D63333738396537663 26
3393200000000042000A070000000F4163746976617469 6F6E2044617465 0042000A07000000114465616374697661746 9
6F6E204461746500000000000000
```

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

Deleted: *300*

Deleted: *300*

Formatted: Font: Courier New, 8 pt, Font color: Black

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11
14:04:00 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-
c3789e7f2c92
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000049E87DC6 (Fri
Apr 17 15:01:58 CEST 2009)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004BC9B1BE (Sat
Apr 17 15:03:58 CEST 2010)
```

```
42007B010000011842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000420092090000000800000004B74004042000D0200000004000000010000000042000F01000000C042
005C05000000040000000B0000000042007F050000000400000000000000042007C01000000984200940700000024333
8393630326231 2D636130322D346333632D623561332D63333738396537663263393200000000420008010000002842 00
0A070000000F41637469766174696F6E204461746500 42000B090000000800000000 49E87DC6420008010000003042000
A070000001144656163746976617469 6F6E204461746500000000000000 42000B09000000080000000004BC9B1BE
```

6	Get Attribute

In: uuidNewKey, attributeName={'State'}

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-
c3789e7f2c92
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000005842005C0500000004000000000B0000000042
00790100000040420094070000002433383936303262312D636130322D346333632D623561332D63333738396537663262
3393200000000042000A070000000553746174650000000
```

Out: uuidNewKey, attribute={ State='*Active*' }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11
14:04:00 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-
c3789e7f2c92
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active)
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004B74004042000D0200000004000000010000000042000F010000008042
005C0500000004000000000B000000000042007F0500000004000000000000000042007C01000000584200940700000024333
83936303262312D636130322D346333632D623561332D633337383965376632633932000000000420008010000002042000
0A070000000553746174650000000042000B05000000040000000200000000
```

7 Destroy

In: uuidKey

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

Formatted: Font: Courier New, 8 pt, Font color: Black

```
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-
0575a41d93b6

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000001400000000042
0079010000003042009407000000246662633566336535 2D343862662D343239342D623735342D30353735613431643933
3623600000000
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11
14:04:00 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbc5f3e5-48bf-4294-b754-
0575a41d93b6

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004B74004042000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F0500000004000000000000000042007C010000003042009407000000024666
26335663365352D343862662D343239342D623735342D30353735613431643933623600000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

8 Destroy

In: uuidNewKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 389602b1-ca02-4c3c-b5a3-
c3789e7f2c92
```

Formatted: Font: Courier New, 8 pt, Font color: Black

	42007801000000904200770100000038420069010000002042006A020000000400000001000000000042006B02000000040
	000000000000000042000D020000000400000001000000000042000F010000004842005C0500000004000000140000000042
	00790100000030420094070000002433383936303262312D636130322D346333632D623561332D6333373839653766326
	3393200000000
	
	Out: uuidNewKey
	
	`Tag: Response Message (0x42007B), Type: Structure (0x01), Data:`
	`  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:`
	`    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)`
	`    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B740040 (Thu Feb 11 14:04:00 CET 2010)`
	`    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:`
	`    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 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: 389602b1-ca02-4c3c-b5a3-c3789e7f2c92`
	
	42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000000042006B02000000040
	00000000000000042009209000000080000000004B74004042000D0200000004000000010000000042000F010000005842
	005C0500000004000000140000000042007F0500000004000000000000000042007C01000000304200940700000024333
	83936303262312D636130322D346333632D623561332D63333738396537663263393200000000

Formatted: Font: Courier New, 8 pt, Font color: Black

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=’*<NOW>*’}
	
	`Tag: Request Message (0x420078), Type: Structure (0x01), Data:`
	`  Tag: Request Header (0x420077), Type: Structure (0x01), Data:`
	`    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)`
	`    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:`
	`    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)`

Formatted: Font: Italic

Deleted: *2*

Formatted: Font: Courier New, 8 pt, Font color: Black

```
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt,
Decrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
          Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B741047 (Thu
Feb 11 15:12:23 CET 2010)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
```

```
42007801000001904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000014842005C050000000400000001000000042
00790100000130420057050000000400000002000000004200910100000118420008010000003042000A0700000017437
27970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200
0A07000000144372797074F677261706869632204C656E677468000000042000B02000000040000008000000000042000
801000000304200 0A0700000018437279707 46F677261706869632055736167652 04D61736B42000B020000000 4000000
0C0000000042000801000000284200 0A070000000F41637469766174696F6E20446174650042000B090000000800000000
04B741047420008010000003842000A07000000044E616D65000000000042000B010000002042005507000000087 2656B65
794B6579420054050000000400000001000000000
```

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: 0x000000004B741048 (Thu Feb 11
15:12:24 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-
53189c79f781
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004B74104842000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F0500000004000000000000000042007C0100000040420057050000000004000
000020000000042009407000000246565613734326234 2D393665642D343233382D616664322D35333138396337396637
383100000000
```

1 Get Attribute

In: uuidKey, attributeName={‘State’}

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

42007801000000A042007701000000384200690100000020420 06A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000005842005C0500000004000000 0B0000000042
00790100000040420094070000002465656137343262342D393665642D343233382D616664322D3533313839633739663
7383100000000042000A07000000055374617465000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

Out: uuidKey, attribute={ State=‘*Active*’ }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data: 
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data: 
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: 
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741048 (Thu Feb 11
15:12:24 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: 
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: 
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-
53189c79f781
      Tag: Attribute (0x420008), Type: Structure (0x01), Data: 
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active)

42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004B74104842000D0200000004000000010000000042000F010000008042
005C0500000004000000 0B0000000042007F0500000004000000000000000042007C0100000058420094070000002465 6
5613734326234 2D393665642D343233382D616664322D3533313839633739663738310000000004200080100000020420 0
0A07000000055374617465000000042000B05000000040000000200000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

2 Revoke (symmetric key as compromised)

In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceDate=*'<NOW>'*

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-
53189c79f781
      Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:
        Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000002 (Key
Compromise)
      Tag: Compromise Occurrence Date (0x420021), Type: Date-Time (0x09), Data:
0x000000004B741048 (Thu Feb 11 15:12:24 CET 2010)
```

```
42007801000000B84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F010000007042005C050000000400000013000000000042
00790100000058420094070000002465656137343262342D393665642D343233382D616664322D3533313839633739663
73831000000004200810100000010420082050000000400000002000000004200210900000008000000004B741048
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11
15:12:25 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-
53189c79f781
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004B74104942000D0200000004000000010000000042000F010000005842
005C0500000004000000130000000042007F0500000004000000000000000042007C01000000304200940700000024656
56137343262342D393665642D343233382D616664322D35333138396337396637383100000000
```

3 Get Attribute

In: uuidKey, attributeName={'State'}

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

Deleted: *6*

Formatted: Font: Italic

Formatted: Font: Courier New, 8 pt, Font color: Black

Formatted: Font: Courier New, 8 pt, Font color: Black

Formatted: Font: Courier New, 8 pt, Font color: Black

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

```
42007801000000A042007701000000384200690100000020042006A02000000040000000100000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F01000000058420005C05000000040000000B0000000042
00790100000040420094070000002465656137343262342D393665642D343233382D616664322D3533313839633739663
738310000000042000A07000000055374617465000000
```

Out: uuidKey, attribute={ State='*Compromised*' }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11
15:12:25 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-
53189c79f781
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (Compromised)
```

```
42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004B74104942000D0200000004000000010000000042000F010000008042
005C0500000004000000B0000000042007F0500000004000000000000000042007C010000005842009407000000024656
56137343262342D393665642D343233382D616664322D35333138396337396637383100000000420008010000002042000
0A07000000055374617465000000042000B050000000400000004000000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

4

Rekey

In: uuidKey

Deleted: , offset='0'

```
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)
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-
53189c79f781

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000040000000042
00790100000030420094070000002465656137343262342D393665642D343233382D616664322D3533313839633739663
7383100000000
```

Out: uuidNewKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11
15:12:25 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-
6ea36a801824

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000000420092090000000800000004B74104942000D0200000004000000010000000042000F010000005842
005C0500000004000000040000000042007F0500000004000000000000000042007C01000000304200940700000024616
43363623737342D643030642D343539312D613633342D366561333661383031383234000000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

5 Get Attribute

In: uuidNewKey, attributeName={‘State’}

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-
6ea36a801824
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000000042000D0200000004000000010000000042000F010000005842005C050000000400000000B0000000042
00790100000040420094070000002461643363623737342D643030642D343539312D613633342D36656133366138303313
832340000000042000A07000000055374617465000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

Out: uuidNewKey, attribute={ State=‘*Active*’ }

Formatted: Font: Courier New, 8 pt, Font color: Black

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11
15:12:25 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-
6ea36a801824
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Active)

42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400
00000000000000042009209000000080000000004B74104942000D0200000004000000010000000042000F010000008042
005C05000000040000000B0000000042007F0500000004000000000000000042007C01000000584200940700000024616
4336362373734 2D643030642D343539312D613633342D36656133366138303138323400000000420008010000002004200
0A07000000055374617465000000420000B0500000004000000020000000 0
```

6 Destroy

In: uuidKey

Formatted: Font: Courier New, 8 pt, Font color: Black

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-
53189c79f781

420078010000009042007701000000384200690100000020042006A0200000004000000010000000042006B0200000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000001400000000042
0079010000003042009407000000246565613734326234 2D393665642D343233382D616664322D3533313839633739663
7383100000000
```

Out: uuidKey

Formatted: Font: Courier New, 8 pt, Font color: Black

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11
15:12:25 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: eea742b4-96ed-4238-afd2-
53189c79f781

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B74104942000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F0500000004000000000000000042007C01000000304200940700000024656
56137343262342D393665642D343233382D616664322D3533313839633739663738310000000
```

7

Destroy

In: uuidNewKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-
6ea36a801824

4200780100000090420077010000003842006901000000202042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000001400000000042
0079010000003042009407000000246164336362373734 2D643030642D343539312D613633342D36656133366138303133
8323400000000
```

Formatted: Font: Courier New, 8 pt, Font color: Black

Out: uuidNewKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B741049 (Thu Feb 11
15:12:25 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ad3cb774-d00d-4591-a634-
6ea36a801824


42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000000042006B02000000040
000000000000000420092090000000800000000 4B74104942000D02000000040000000100000000042000F010000005842
005C050000000400000014000000000042007F05000000040000000000000000042007C0100000030420094070000002461 6
4336362373734 2D643030642D343539312D613633342D36656133366138303138323400000000
```

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.

<table>
<tr><th>Time</th><th>Client A</th></tr>
<tr><td>0</td><td>Create (symmetric key)
In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='rekeyKey', NameType='00000001' } }<pre>
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt,
Decrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
</pre></td></tr>
</table>

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007801000001604200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000042000D0200000004000000010000000042000F010000011842005C0500000004000000010000000042
007901000001004200570500000004000000020000000042009101000000E842000801000000304200A0700000017437
27970746F67726170686963204l6C676F726974686D0042000B0500000004000000030000000042000801000000304200
0A07000000144372797074667261706869632C656E677468000000000042000B0200000004000000080000000042000
801000000304200A0700000018437279707467261706869632055736167652D61736B42000B0200000004000000
0C00000000420008010000003842000A07000000044E616D650000000042000B0100000020420055070000000872656B6
5794B6579420054050000000400000001000000000
```

Out: objectType='00000002', uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742475 (Thu Feb 11
16:38:29 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-
4d6fc85a56ef
```

Formatted: Font: 8 pt, Font color: Black

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000042009209000000080000000004B74247542000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F0500000004000000000000000042007C010000004042005705000000004000
00002000000004200940700000024663033343235393020D663738612D346433342D613266342D34643666633835613536
656600000000
```

1 Locate

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

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

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007801000000A0420077010000003842006901000000204200 6A0200000004000000010000000042006B02000000040
000000000000042000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042
```

```
0079010000000404200080100000003842000A07000000044E616D650000000042000B01000000204200550700000008726
56B65794B657942005405000000040000000100000000
```

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: 0x000000004B742476 (Thu Feb 11
16:38:30 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-
4d6fc85a56ef
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
0000000000000004200920900000008000000004B74247642000D02000000040000000100000000042000F010000005842
005C05000000040000000800000000042007F05000000040000000000000000042007C01000000304200940700000024663
03334323539302D663738612D346433342D613266342D346436666338356135366566600000000
```

2

Rekey

In: uuidKey, attributes={ ActivationDate=’0000000043B7B630’, ProcessStartDate=’0000000043B7B630’, ProtectStopDate=’000000005E0C7BB0’, DeactivationDate=’000000005E0C7BB0’ }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-
4d6fc85a56ef
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
          Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000043B7B630 (Sun
Jan 01 12:00:00 CET 2006)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Process Start Date
          Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000043B7B630 (Sun
Jan 01 12:00:00 CET 2006)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date
          Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000005E0C7BB0 (Wed
```

Formatted: Font: Courier New, 8 pt, Font color: Black

```
Jan 01 12:00:00 CET 2020)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date
          Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000005E0C7BB0 (Wed
Jan 01 12:00:00 CET 2020)
```

```
42007801000001704200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F010000012842005C0500000004000000040000000042
007901000001104200940700000024663033343235393O2D663738612D346433342D613266342D34643666633835613533
```

Out: uuidNewKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742477 (Thu Feb 11
16:38:31 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-
ff6ffaa75fbd
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B74247742000D0200000004000000010000000042000F010000005842
005C0500000004000000040000000042007F0500000004000000000000000042007C010000003042009407000000024613
366613665356322D313339372D346162342D396431322D66663666666161373566626400000000
```

3 Get Attribute

In: uuidKey, attributeName={'Name'}

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-
4d6fc85a56ef
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
```

Formatted: Font: Courier New, 8 pt

Formatted: Font: Courier New, 8 pt

```
42007801000000A04200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F01000000584200 5C0500000004000000000B0000000042
0079010000004042009407000000246630333432353930 2D663738612D346433342D613266342D3464366663383561353
665660000000042000A07000000044E616D6500000000
```

Out: uuidKey

Deleted: Operation Failed, Item Not Found

Formatted: Font: Courier New, 8 pt

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742477 (Thu Feb 11
16:38:31 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-
4d6fc85a56ef

42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000420092090000000080000000004B74247742000D0200000004000000010000000042000F010000005842
005C0500000004000000000B000000000042007F0500000004000000000000000042007C0100000030420094070000024663
03334323539302D663738612D346433342D613266342D34643666633835613536656600000000
```

4

Get Attribute

In: uuidKey, attributeName={ ‘ActivationDate’, ‘ProcessStartDate’, ‘ProtectStopDate’, ‘DeactivationDate’ }

Formatted: Font: Courier New, 8 pt

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-
ff6ffaa75fbd
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Process Start Date
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date

42007801000001084200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F01000000C042005C0500000004000000000B0000000042
00790100000A842009407000000246133666136653632D313339372D346162342D396431322D6666366666616137356
6626400000000042000A070000000F416374697661746696F6E204461746500 42000A0700000001250726F63657373205374
617274204461746500000000000042000A070000001150726F7465637420537 46F7020446174650000000000000042000
A07000000114465616374697661746 96F6E20446174650000000000000000
```

Out: uuidKey, attribute={ ActivationDate='0000000043B7B630', ProcessStartDate='0000000043B7B630', ProtectStopDate='000000005E0C7BB0', DeactivationDate='000000005E0C7BB0' }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742477 (Thu Feb 11
16:38:31 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-
ff6ffaa75fbd
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000043B7B630 (Sun
Jan 01 12:00:00 CET 2006)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Process Start Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x0000000043B7B630 (Sun
Jan 01 12:00:00 CET 2006)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Protect Stop Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000005E0C7BB0 (Wed
Jan 01 12:00:00 CET 2020)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Deactivation Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000005E0C7BB0 (Wed
Jan 01 12:00:00 CET 2020)
```

Formatted: Font: Courier New, 8 pt

```
42007B01000001884200７A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
```

5 Locate

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

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

Formatted: Font: Courier New, 8 pt

```
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey
          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)

42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042
00790100000040420008010000003842000A07000000044E616D650000000042000B010000002042005507000000008726
56B65794B65794200540500000004000000010000000
```

Out: uuidNewKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742477 (Thu Feb 11 16:38:31 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004B74247742000D0200000004000000010000000042000F010000005842
005C0500000004000000080000000042007F0500000004000000000000000042007C010000003042009407000000024613
36661366535632D313339372D346162342D396431322D66663666666161373566626400000000
```

Formatted: Font: Courier New, 8 pt

6 Destroy

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-4d6fc85a56ef
```

Formatted: Font: Courier New, 8 pt

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000000042000D0200000004000000010000000042000F01000000484200 5C0500000004000000140000000042
0079010000003042009407000000246630333432353930 2D663738612D346433342D613266342D346436666338356135 3
6656600000000
```

Out: uuidKey

Formatted: Font: Courier New, 8 pt

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742478 (Thu Feb 11
16:38:32 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: f0342590-f78a-4d34-a2f4-
4d6fc85a56ef
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042009209000000080000000004B74247842000D0200000004000000010000000042000F01000000 5842
005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002466 3
03334323539302D663738612D346433342D613266342D34643666633835613536656600000000
```

7 Destroy

In: uuidNewKey

Formatted: Font: Courier New, 8 pt

```
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: a3fa6e5c-1397-4ab4-9d12-
ff6ffaa75fbd
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000000042000D0200000004000000010000000042000F01000000484200 5C0500000004000000140000000042
0079010000003042009407000000246133666136653563 2D313339372D346162342D396431322D666636666661613735 6
6626400000000
```

Out: uuidNewKey

Formatted: Font: Courier New, 8 pt

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

	Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B742478 (Thu Feb 11 16:38:32 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: a3fa6e5c-1397-4ab4-9d12-ff6ffaa75fbd 42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040 000000000000000420092090000000800000000004B74247842000D0200000004000000010000000042000F010000005842 005C0500000004000000140000000042007F0500000004000000000000000042007C010000003042009407000000024613 36661366535632D313339372D346162342D396431322D666636666661613735666264400000000

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
0	Client A: Create (symmetric key) In: objectType=’00000002’, attributes={ CryptographicAlgorithm=’AES’, CryptographicLength=’128’, CryptographicUsageMask=‘0000000C’, Name={ NameValue=‘ rekeyKey’, NameType=’00000001’ }, ActivationDate=’*<NOW>*’ } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data: Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)

Deleted: A

Formatted Table

Deleted: *2*

Formatted: Font: Italic

Formatted: Font: Courier New, 8 pt

```
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt,
Decrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: rekeyKey
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Activation Date
          Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B74262C (Thu
Feb 11 16:45:48 CET 2010)
```

```
420078010000019042007701000000384200690100000020420006A0200000004000000010000000042006B02000000040
00000000000000042000D02000000040000000100000000042000F010000014842005C050000000400000001000000042
00790100000130420057050000000400000002000000004200910100000118420008010000003042000A0700000017437
27970746F6772617068696320416C676F726974686D0042000B050000000400000003000000004200080100000304200
0A070000001443727970746F67726170686963204C656E6774680000000042000B020000000400000080000000042000
80100000030420000A070000001843727970746F67726170686963205573616765204D61736B42000B0200000004000000
0C000000004200080100000038420000A07000000044E616D650000000042000B010000002042005507000000872656B6
5794B657942005405000000040000000100000000420008010000002842000A070000000F41637469766174696F6E2044
6174650042000B09000000080000000004B74262C
```

Out: objectType=’00000002’, uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262D (Thu Feb 11
16:45:49 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-
262895bc31ce
```

Formatted: Font: 8 pt

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B74262D42000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F0500000004000000000000000042007C010000004042005705000000040000
00020000000042009407000000246361333638653332D646333642D346337632D386636642D32363238393562633331
636500000000
```

1 Client A:

Get (symmetric key)

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-
262895bc31ce
```

Formatted: Font: Courier New, 8 pt

```
420078010000009042007701000000384200690100000020420006A02000000040000000100000000042006B02000000040
0000000000000000042000D0200000004000000010000000042000F0100000048420005C050000000400000000A0000000042
007901000000304200940700000024636133363865333332D646333642D346337632D386636642D3236323839356263333
1636500000000
```

Out: objectType = ‘00000002’, uuidKey, symmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262D (Thu Feb 11
16:45:49 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-
262895bc31ce
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data:
F43C7798AACB22B1411A8773C199708B
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003
(AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
```

Formatted: Font: Courier New, 8 pt

```
42007B010000012042007A010000004842006901000000204200 6A02000000040000000100000000042006B02000000040
00000000000000004200920900000008000000004B74262D42000D020000000400000001000000042000F01000000C842
005C050000000400000000A000000000042007F050000000400000000000000042007C01000000A0420057050000000004000
000020000000042009407000000024636133363865333332D646333642D346337632D386636642D32363238393562633331
6365000000000042008F010000005842004001000000504200420500000004000000010000000420045010000001842004
30800000010F43C7798AACB22B1411A8773C199708B420028050000000400000003000000042002A02000000004000000
8000000000
```

2 Client A:

Obtain Lease

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-
262895bc31ce
```

Formatted: Font: Courier New, 8 pt

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000010000000000042
00790100000030420094070000002463613336386533332D646333642D346337632D386636642D3236323839356263333
1636500000000
```

Out: uuidKey, leaseTime, lastChangeDate

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262E (Thu Feb 11
16:45:50 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-
262895bc31ce
      Tag: Lease Time (0x420049), Type: Interval (0x0A), Data: 0x00000010
      Tag: Last Change Date (0x420048), Type: Date-Time (0x09), Data: 0x000000004B74262D (Thu Feb
11 16:45:49 CET 2010)
```

Formatted: Font: Courier New, 8 pt

```
42007B01000000D042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B74262E42000D0200000004000000010000000042000F010000007842
005C050000000400000010000000000042007F0500000004000000000000000042007C010000005042009407000000024636
13336386533332D646333642D346337632D386636642D323632383935626333316365000000004200490A000000040000
00100000000042004809000000080000000004B74262D
```

3

Client B:

Revoke (symmetric key as compromised)

In: uuidKey, RevocationReason='00000002', CompromiseOccurrenceDate='*<NOW>*'

Formatted: Font: Italic

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

Formatted: Font: Courier New, 8 pt

```
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-
262895bc31ce
      Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:
        Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000002 (Key
Compromise)
      Tag: Compromise Occurrence Date (0x420021), Type: Date-Time (0x09), Data:
0x000000004B74262E (Thu Feb 11 16:45:50 CET 2010)

42007801000000B84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000007042005C050000000400000013000000042
0079010000005842009407000000246361333638653332D646333642D346337632D386636642D3236323839356263333
163650000000042008101000000104200820500000004000000020000000042002109000000080000000004B74262E
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262E (Thu Feb 11
16:45:50 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-
262895bc31ce

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042009209000000080000000004B74262E42000D0200000004000000010000000042000F01000000005842
005C050000000400000013000000042007F0500000004000000000000000042007C010000003042009407000000024636
1333638653332D646333642D346337632D386636642D323632383935626333316365000000000
```

Formatted: Font: Courier New, 8 pt

4

Client B:

Rekey

In: uuidKey

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

Formatted: Font: Courier New, 8 pt

```
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce

420078010000009042007701000000384200690100000020420006A02000000040000000100000000042006B02000000040000000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000004000000000420079010000003042009407000000246361333638653332D646333642D346337632D386636642D32363238393562633331636500000000
```

Out: uuidNewKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f

42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042006B020000000400000000000000000420092090000000080000000004B74262F42000D0200000004000000010000000042000F010000005842005C0500000004000000040000000042007F0500000004000000000000000042007C010000003042009407000000243539666266383164D353734662D346634662D393538312D373738356463353933663566600000000
```

Formatted: Font: Courier New, 8 pt

5 Client A:

Obtain Lease

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce

420078010000009042007701000000384200690100000020420006A02000000040000000100000000042006B02000000040000000000000000042000D0200000004000000010000000042000F010000004842005C0500000004000000100000000042
```

Formatted: Font: Courier New, 8 pt

```
0079010000000304200940700000002463613336386533332D646333642D346337632D386636642D32363238393562633331636500000000
```

Out: Operation Failed, Permission Denied

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)
    Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x0000000C (Permission Denied)
    Tag: Result Message (0x42007D), Type: Text String (0x07), Data: CO is in state Compromised, no lease given
```

Formatted: Font: Courier New, 8 pt

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004B74262F42000D0200000004000000010000000042000F010000006842
005C0500000004000000100000000042007F0500000004000000010000000042007E050000000400000000C00000000420
07D070000002A434F20697320696E207374617465436F6D70726F6D697365642C206E6F206C656173652067697665 6E
000000000000
```

6

Client A:

Locate (symmetric key)

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

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

Formatted: Font: Courier New, 8 pt

```
42007801000000A042007701000000384200690100000020420 06A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000000058420 05C0500000004000000080000000042
00790100000040420008010000003842000A07000000044E616D650000000042000B01000000204200550700000008726
56B65794B6579420054050000000400000001000000000
```

Out: uuidNewKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11
16:45:51 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-
7785dc593f5f
```

Formatted: Font: Courier New, 8 pt

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B74262F42000D0200000004000000010000000042000F010000005842
005C0500000004000000080000000042007F0500000004000000000000000042007C010000003042009407000000024353
96662663831642D353734662D346634662D393538312D37373835646335393366356600000000
```

7 Client A:

Get (symmetric key)

In: uuidNewKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-
7785dc593f5f
```

Formatted: Font: Courier New, 8 pt

```
420078010000009042007701000000384200690100000020042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000000A0000000042
0079010000003042009407000000243539666266383164 2D353734662D346634662D393538312D37373835646335393336
6356600000000
```

Out: objectType = ‘00000002’, uuidNewKey, newSymmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11
```

Formatted: Font: Courier New, 8 pt

	16:45:51 CET 2010) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data: Tag: Key Block (0x420040), Type: Structure (0x01), Data: Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001 Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Octet String (0x08), Data: 173E9499F7C573712AFB9883B5DF2BCE Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128) 42007B01000001204200 7A0100000048420069010000002042006A02000000040000000100000000 42006B02000000040 0000000000000004200920900000008000000004B74262F42000D0200000004000000010000000042000F01000000C842 005C0500000004000000 0A0000000042007F05000000040000000000000000 42007C01000000A04200570500000004000 00002000000004200940700000024353966626638316 42D353734662D346634662D393538312D37373835646335393366 35660000000042008F010000005842004001000000504200420500000004000000010000000042004501000000184200 4 308000000 10173E9499F7C573712AFB9883B5DF2BCE42002805000000040000000300000000 42002A02000000040000 00 8000000000
8	Client A: Obtain Lease In: uuidNewKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040 0000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000010000000042 007901000000304200940700000024353966626638316 42D353734662D346634662D393538312D3737383564633539336 6356600000000 Out: uuidNewKey, leaseTime, lastChangeDate Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

Formatted: Font: Courier New, 8 pt

Formatted: Font: Courier New, 8 pt

```
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-7785dc593f5f
      Tag: Lease Time (0x420049), Type: Interval (0x0A), Data: 0x00000000
      Tag: Last Change Date (0x420048), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)
```

```
42007B01000000D042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000420092090000000080000000004B74262F42000D02000000040000000100000000042000F010000007842
005C050000000040000000100000000042007F050000000040000000000000000042007C010000005042009407000000024353
96662663831642D353734662D346634662D393538312D373738356463353933663566000000004200490A000000040000
000000000000420048090000000080000000004B74262F
```

9

Client A:

Destroy

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-262895bc31ce
```

Formatted: Font: Courier New, 8 pt

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000042000D02000000040000000100000000042000F010000004842005C050000000400000014000000042
0079010000003042009407000000246361333638653332D646333642D346337632D386636642D3236323839356263333
1636500000000
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11 16:45:51 CET 2010)
```

Formatted: Font: Courier New, 8 pt

```
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ca368e33-dc3d-4c7c-8f6d-
262895bc31ce
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000420092090000000080000000004B74262F42000D0200000004000000010000000042000F010000005842
005C050000000400000014000000000042007F0500000004000000000000000042007C0100000030420094070000002463 6
13336386533332D646333642D346337632D386636642D32363238393562633331636500000000
```

10

Client A:

Destroy

In: uuidNewKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 59fbf81d-574f-4f4f-9581-
7785dc593f5f
```

Formatted: Font: Courier New, 8 pt

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000000042
00790100000030420094070000002435396662663831642D353734662D346634662D393538312D37373835646335393336
6356600000000
```

Out: uuidNewKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B74262F (Thu Feb 11
16:45:51 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 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: 59fbf81d-574f-4f4f-9581-
7785dc593f5f
```

Formatted: Font: Courier New, 8 pt

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
```

<table>
<tr><td></td><td><pre>
0000000000000004200920900000000800000000004B74262F42000D0200000000400000001000000000042000F010000005842
005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002435 3
96662663831642D353734662D346634662D393538312D37373835646335393366356600000000
</pre></td></tr>
</table>

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.

<table>
<tr><th>Time</th><th>Client A</th></tr>
<tr><td>0</td><td>Create (symmetric key)
In: objectType=’00000002’, attributes={ CryptographicAlgorithm=’AES’, CryptographicLength=’128’, CryptographicUsageMask=‘0000000C’, Name={ NameValue=‘archiveKey’, NameType=’00000001’ } }<pre>
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt,
Decrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
</pre></td></tr>
</table>

Formatted: Font: Courier New, 8 pt

```
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: archiveKey
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted text string)
```

```
42007801000001684200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000042000D0200000004000000010000000042000F010000012042005C0500000004000000010000000042
007901000001084200570500000004000000020000000042009101000000F042000801000000304200A070000000174 37
27970746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000000304200
0A0700000014437279707465F6772617068963204C656E6774680000000042000B020000000400000080000000042000
801000000304200A07000000018437279707465F677261706869632055736167652044D61736B42000B02000000004000000
0C000000004200080100000004042000A07000000044E616D650000000042000B010000002842005507000000A6172636
86976654B65790000000000004200540500000004000000100000000
```

Out: objectType='00000002', uuidKey

Formatted: Font: 8 pt

```
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: 0x000000004B751FA3 (Fri Feb 12 10:30:11 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
```

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000004200920900000008000000004B751FA342000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F05000000040000000000000000042007C010000004042005705000000004000
00002000000004200940700000024306435353231363 02D666230342D346637632D386137332D6665663930356232316 3
306600000000
```

1 Locate

In: attributes={ Name={ NameValue='archiveKey', NameType='00000001' } }

Formatted: Font: Courier New, 8 pt

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

42007801000000D84200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000000904200 5C050000000400000008000000042
00790100000078420008010000002842000A070000000B4F626A6563742054797065000000000042000B0500000004000
000020000000042000801000000404200 0A07000000044E616D650000000042000B010000002842005507000000 0A6172
63686976654B65790000000000000420054050000000400000001000000000
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FA6 (Fri Feb 12
10:30:14 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-
fef905b21c0f

42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
00000000000000004200920900000008000000004B751FA642000D0200000004000000010000000042000F010000005842
005C0500000004000000080000000042007F0500000004000000000000000042007C01000000304200940700000024306
43535323136302D666230342D346637632D386137332D6665663930356232316330660000000
```

Formatted: Font: Courier New, 8 pt

2 Get (symmetric key)

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-
fef905b21c0f

42007801000000904200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000000484200 5C05000000040000000A000000042
0079010000003042009407000000243064353532313630 2D666230342D346637632D386137332D6665663930356232316
```

Formatted: Font: Courier New, 8 pt

```
3306600000000
```

Out: objectType = ‘00000002’, uuidKey, symmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FA7 (Fri Feb 12
10:30:15 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-
fef905b21c0f
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data:
C3200B1291BA648DB9089DED3073DE74
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003
(AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
```

Formatted: Font: Courier New, 8 pt

```
42007B010000012042007A01000000484200690100000020042006A02000000040000000100000000042006B02000000040
000000000000000420092090000000800000000 4B751FA742000D0200000004000000010000000042000F01000000C842
005C05000000040000000A0000000042007F0500000004000000000000000042007C01000000A04200570500000004000
00002000000004200940700000024306435353231363 02D666230342D346637632D386137332D66656639303562323163
30660000000042008F01000000584200400100000050420042050000000400000001000000004200450100000018 42004
30800000010C3200B1291BA648DB9089DED3073DE74420028050000000400000003000000004 2002A0200000004000000
8000000000
```

3 Archive

In: uuidKey, asynchronousIndicator=’true’

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000015 (Archive)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-
fef905b21c0f
```

Formatted: Font: Courier New, 8 pt

```
42007801000000A04200770100000048420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000420007060000000800000000000000001420000D020000000400000001000000004200F010000004842
005C0500000004000000150000000042007901000000304200940700000024306435353231363020D666230342D3466376
32D386137332D66656639303562323163306600000000
```

Out: asynchronousCorrelationValue

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FA7 (Fri Feb 12
10:30:15 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000015 (Archive)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Operation Pending)
    Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:
F17893DB51652969
```

Formatted: Font: Courier New, 8 pt

```
42007B010000008842007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000420092090000000800000000004B751FA742000D02000000040000000100000000042000F010000003042
005C050000000400000015000000004200 7F05000000040000000200000000420006080000000 8F17893DB51652969
```

4 Poll*

In: asynchronousCorrelationValue

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:
F17893DB51652969
```

Formatted: Font: Courier New, 8 pt

```
42007801000000704200770100000038420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000002842005C05000000040000001A0000000042
007901000000104200060800000008F17893DB51652969
```

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)
```

Formatted: Font: Courier New, 8 pt

```
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAA (Fri Feb 12
10:30:18 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000015 (Archive)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-
fef905b21c0f
```

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B751FAA42000D0200000004000000010000000042000F010000005842
005C05000000040000001500000000042007F0500000004000000000000000042007C010000003042009407000000024306
43535323136302D666230342D346637632D386137332D66656639303562323163306600000000

5 Get (symmetric key)

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-
fef905b21c0f
```

Formatted: Font: Courier New, 8 pt

42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000000484200 5C0500000004000000 0A0000000042
00790100000030420094070000002430643535323136302D666230342D346637632D386137332D666566393035623231 6
3306600000000

Out: Operation Failed, Object Archived

Deleted: 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: 0x000000004B751FAC (Fri Feb 12
10:30:20 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)
    Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x0000000D (Object Archived)
    Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Object is archived
```

Formatted: Font: Courier New, 8 pt

	42007B01000000A842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040 000000000000000420092090000000080000000004B751FAC42000D0200000004000000010000000042000F010000005042 005C0500000004000000000A0000000042007F0500000004000000010000000042007E0500000004000000000D00000000420 07D07000000124F626A65637420697320617263686976656400000000000000

6	Get Attribute (Archive Date)
	In: uuidKey, attributeName='ArchiveDate'
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
	    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
	      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Archive Date
	
	42007801000000A84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
	00000000000000042000D0200000004000000010000000042000F010000006042005C0500000004000000000B0000000042
	0079010000004842009407000000243064353532313630 2D666230342D346637632D386137332D6665663930356232316
	33066000000000042000A070000000C4172636869766520446174650000000
	
	Out: uuidKey, attribute={ ArchiveDate }
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
	    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAC (Fri Feb 12 10:30:20 CET 2010)
	    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
	    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
	      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Archive Date
	        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B751FAA (Fri Feb 12 10:30:18 CET 2010)
	
	42007B01000000E042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
	000000000000000420092090000000080000000004B751FAC42000D0200000004000000010000000042000F010000008842
	005C0500000004000000000B0000000042007F0500000004000000000000000042007C010000006042009407000000024306
	43535323136302D666230342D346637632D386137332D66656639303562323163306600000000420008010000002842000
	0A070000000C417263686976652044617465000000000042000B090000000080000000004B751FAA

7 Locate

Deleted: 6

In: attributes={ Name={ NameValue='archiveKey', NameType='00000001' } }

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

Formatted: Font: Courier New, 8 pt

```
42007801000000D84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000009042005C0500000004000000080000000042
00790100000078420008010000002842000A070000000B4F626A656374205479706500000000000042000B0500000004000
0000200000000420008010000004042000A07000000044E616D650000000042000B01000000284200550700000000A6172
63686976654B6579000000000000004200540500000004000000010000000
```

Out: <empty response payload>

Deleted: 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: 0x000000004B751FAC (Fri Feb 12
10:30:20 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: null
```

Formatted: Font: Courier New, 8 pt

```
42007B010000008042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B751FAC42000D0200000004000000010000000042000F010000002842
005C0500000004000000080000000042007F0500000004000000000000000042007C0100000000
```

8 Locate

Deleted: 7

In: storageStatusMask='00000003', attributes={ Name={ NameValue='archiveKey', NameType='00000001' } }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Storage Status Mask (0x42008E), Type: Integer (0x02), Data: 0x00000003 (3)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric
Key)
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Name Value (0x420055), Type: Text String (0x07), Data: archiveKey
          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
```

Formatted: Font: Courier New, 8 pt

```
42007801000000E84200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000000A042005C0500000004000000080000000042
0079010000008842008E0200000004000000030000000042000801000000284200A070000000B4F626A6563742054797
0650000000000042000B0500000004000000020000000042000801000000404200A07000000044E616D65000000004200
0B01000000284200550700000000A617263686976654B657900000000000004200540500000004000000010000000
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAC (Fri Feb 12
10:30:20 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-
fef905b21c0f
```

Formatted: Font: Courier New, 8 pt

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000004200920900000008000000004B751FAC42000D0200000004000000010000000042000F010000005842
005C0500000004000000080000000042007F0500000004000000000000000042007C010000003042009407000000024306
43535323136302D666230342D346637632D386137332D66656639303562323163306600000000
```

9 Recover

In: uuidKey, asynchronousIndicator='true'

Deleted: 8

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Asynchronous Indicator (0x420007), Type: Boolean (0x06), Data: TRUE
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000016 (Recover)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-
fef905b21c0f
```

```
42007801000000A0420077010000004842006901000000204200 6A0200000004000000010000000042006B02000000040
```

Out: asynchronousCorrelationValue

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FAC (Fri Feb 12
10:30:20 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000016 (Recover)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000002 (Operation Pending)
    Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data:
DDBB075607727F3F
```

```
42007B010000008842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000000 4B751FAC42000D0200000004000000010000000042000F010000003042
005C05000000040000001600000000 42007F0500000004000000020000000042000608000000 08DDBB075607727F3F
```

10 Poll*

In: asynchronousCorrelationValue

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
```

Formatted: Font: Courier New, 8 pt

Formatted: Font: Courier New, 8 pt

Deleted: 9

Formatted: Font: Courier New, 8 pt

```
      Tag: Asynchronous Correlation Value (0x420006), Type: Octet String (0x08), Data: 
DDBB075607727F3F
```

```
42007801000000704200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F01000000028420005C0500000004000000001A0000000042
007901000000010420006080000008DDBB075607727F3F
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data: 
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data: 
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: 
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FB3 (Fri Feb 12 
10:30:27 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: 
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000016 (Recover)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: 
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-
fef905b21c0f
```

Formatted: Font: Courier New, 8 pt

```
42007B01000000B042007A01000000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000000420092090000000800000004B751FB342000D0200000004000000010000000042000F010000005842
005C05000000040000001600000000042007F0500000004000000000000000042007C01000000304200940700000024306
43535323136302D666230342D346637632D386137332D6665663930356232316330660000000
```

11 Get (symmetric key)

Deleted: 10

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data: 
  Tag: Request Header (0x420077), Type: Structure (0x01), Data: 
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: 
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: 
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data: 
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-
fef905b21c0f
```

Formatted: Font: Courier New, 8 pt

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000000042000D0200000004000000010000000042000F01000000048420005C0500000004000000000A0000000042
007901000000304200940700000024306435353231363 02D666230342D346637632D386137332D666566393035623231 6
3306600000000
```

Out: objectType = ‘00000002’, uuidKey, symmetricKey

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

Formatted: Font: Courier New, 8 pt

```
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FB3 (Fri Feb 12 10:30:27 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
      Tag: Symmetric Key (0x42008F), Type: Structure (0x01), Data:
        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Octet String (0x08), Data: C3200B1291BA648DB9089DED3073DE74
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
```

```
42007B010000012042007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
0000000000000004200920900000008000000004B751FB342000D020000000400000001000000042000F01000000C842
005C05000000040000000A000000042007F05000000040000000000000000042007C01000000A042005705000000004000
00002000000000420094070000002430643535323136302D666230342D346637632D386137332D6665663930356232316 3
3066000000000042008F01000000584200400100000050420042050000000400000001000000004200450100000018420 04
30800000010C3200B1291BA648DB9089DED3073DE744200280500000004000000030000000042002A0200000004000000
8000000000
```

12 Destroy

Deleted: 11

In: uuidKey

Formatted: Font: Courier New, 8 pt

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-fef905b21c0f
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000D0200000004000000010000000042000F010000004842005C05000000040000001400000000042
0079010000003042009407000000243064353532313630 2D666230342D346637632D386137332D666566393035623231 6
3306600000000
```

Out: uuidKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B751FB4 (Fri Feb 12
10:30:28 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 0d552160-fb04-4f7c-8a73-
fef905b21c0f
```

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000004200920900000008000000004B751FB442000D0200000004000000010000000042000F010000005842
005C05000000040000001400000000042007F050000000400000000000000000042007C010000003042009407000000024306
43535323136302D666230342D346637632D386137332D66656639303562323163306600000000

Formatted: Font: Courier New, 8 pt

11 Access Control, Policies

Formatted: Bullets and Numbering

These use-cases test attributes and objects related to access control and server policy.

11.1 Use-case: Credential, Operation Policy, Destroy Date

Formatted: Bullets and Numbering

Pass a Credential object in the message header in all requests for identification purposes (how the Credential object is used is defined in **[KMIP-Prof]**). Create a symmetric key and set the Operation Policy Name attribute to "Default". Using another Credential, attempt to perform a Get operation batched with a Get Atttribute List on the created symmetric key – according to the Default Operation Policy, both these request SHALL fail, and with the Batch Error Continuation Option set to "Continue", the client SHALL also receive both response payloads. Using the initially used Credential, destroy the object and get the Destroy Date attribute.

The message exchanges in this use case are based on a certain server policy (e.g. handling of Credentials) that in some aspects differs from the policy assumed in earlier use cases (e.g. in this use case, the Destroy Date is retained). As mentioned in Section **Error! Reference source not found.**, the message exchanges shown in this document are not the only correct alternatives. The Credentials shows here are only one interpretation of the Username & Password credential type – the exact format of this credential may vary from one system to another.

Time	Request/Response

0	Create (symmetric key)
	In (header): credential={ credentialType='1', credentialValue=''0x43726564656E7469616C413A736563726574' }
	In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', Name={ NameValue='PolicyKey', NameType='00000001' },
	OperationPolicyName='Default', CryptographicParameters={ BlockCipherMode='1', PaddingMethod='3',

HashingAlgorithm='4'} }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Authentication (0x42000C), Type: Structure (0x01), Data:
      Tag: Credential (0x420023), Type: Structure (0x01), Data:
        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001
        Tag: Credential Value (0x420025), Type: Octet String (0x08), Data:
43726564656E7469616C413A736563726574
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080 (128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage
Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C (Encrypt,
Decrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: PolicyKey
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted
text string)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Operation Policy Name
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Default
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic
Parameters
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Block Cipher Mode (0x420011), Type: Enumeration (0x05), Data: 0x00000001 (CBC)
            Tag: Padding Method (0x42005F), Type: Enumeration (0x05), Data: 0x00000003 (PKCS5)
            Tag: Hashing Algorithm (0x420038), Type: Enumeration (0x05), Data: 0x00000004 (SHA-1)
```

```
42007801000002404200770100000078420069010000002042006A02000000040000000100000000042006B02000000040
00000000000000042000C010000003842002301000000304200240500000004000000010000000042002508000001243
726564656E7469616C413A736563726574000000000000042000D02000000040000000100000000042000F01000001B8420
05C0500000004000000010000000042007901000001A04200570500000004000000020000000042009101000001884200
0801000000030420000A070000001743727970746F6772617068696320416C676F726974686D0042000B050000000400000
003000000000420008010000003042000A070000001443727970746F67726170686963204C656E677468000000000042000B
```

```
020000000400000008000000000420008010000003042000A07000000184372797074 6F6772617068696320557361676520
```

```
0200000004000000080000000004200080100000030420 00A0700000018437279707 46F677261706869632055736167652
04D61736B42000B020000000400000000C00000000420008010000004042000A07000000044E616D65000000000042000B01
000000284200550700000009506F6C6963794B65790000000000000000420054050000000400000001000000004200080 10
000003042000A07000000154F7065726174696F6E20506F6C696379204E616D6500000000 42000B07000000074465666175
6C7400420008010000005842000A07000000184372797074 6F6772617068696320506172616D657465727342000B01000
00030420011050000000400000001000000004200 5F0500000004000000030000000042003805000000040000000 40000
0000
```

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: 0x000000004B757910 (Fri Feb 12
16:51:44 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 81d1d04a-e47f-40ec-a48f-
1fca748b976a
```

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004B75791042000D0200000004000000010000000042000F010000006842
005C0500000004000000010000000042007F0500000004000000000000000042007C010000004042005705000000040000
000200000000420094070000002438316431643034612D653437662D343065632D613438662D316663613734386239373
366100000000
```

1

Client A

Get Attributes, Get

In (header): credential={ credentialType='1', credentialValue=''0x43726564656E7469616C413A736563726574' }

In: attributeName='Operation Policy Name'

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Authentication (0x42000C), Type: Structure (0x01), Data:
      Tag: Credential (0x420023), Type: Structure (0x01), Data:
        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001
        Tag: Credential Value (0x420025), Type: Octet String (0x08), Data:
43726564656E7469616C413A736563726574
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BE9B52A3ED964254
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 81d1d04a-e47f-40ec-a48f-
1fca748b976a
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Operation Policy Name
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 64CA2CFEDFEEDDE1
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 81d1d04a-e47f-40ec-a48f-
1fca748b976a
```

```
42007801000001604200770100000078420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000C01000000384200230100000030420024050000000400000001000000004200250800000001243
726564656E7469616C413A73656372657400000000000042000D0200000004000000020000000042000F0100000078420
05C05000000040000000B000000004200930800000008BE9B52A3ED964254420079010000005042009407000000243831
6431643034612D653437662D343065632D613438662D3166636137343862393736610000000042000A07000000154F706
5726174696F6E20506F6C696379204E616D650000000042000F010000005842005C05000000040000000A00000000420093
080000000864CA2CFEDFEEDDE1420079010000003042009407000000243831643164303461 2D653437662D343065632D6
13438662D31666361373438623937366100000000
```

Out: attributes={ OperationPolicyName='Default' }

Out: objectType = '00000002', uuidKey, symmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B757911 (Fri Feb 12
16:51:45 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: BE9B52A3ED964254
    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: 81d1d04a-e47f-40ec-a48f-
1fca748b976a
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Operation Policy Name
        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Default
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 64CA2CFEDFEEDDE1
    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: 81d1d04a-e47f-40ec-a48f-
1fca748b976a
      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:
A8A775BAF6FE14F903E3CD90C15A29EA
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003
(AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
```

```
42007B01000001D842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B7579114200D0200000004000000020000000042000F01000000A042
005C05000000040000000B000000004200930800000008BE9B52A3ED96425442007F05000000040000000000000000420
07C010000006842009407000000243831643164303461 2D653437662D343065632D613438662D31666361373438623937
366100000000420008010000003042000A07000000154F7065726174696F6E20506F6C696379204E616D6500000042000
B070000000744656661756C740042000F01000000D842005C05000000040000000A000000004200930800000008 64CA2C
FEDFEEDDE142007F05000000040000000000000000042007C01000000A042005705000000040000000200000000 4200940
70000002438316431643034612D653437662D343065632D613438662D31666361373438623937366100000000 42008F01
0000005842000400100000005042004205000000040000000100000000420045010000001842004308000000010A8A775BAF
6FE14F903E3CD90C15A29EA42002805000000040000000300000000042002A02000000040000008000000000
```

2 Client B

Get (symmetric key), Get Attribute List

In (header): credential={ credentialType='1', credentialValue=''0x43726564656E7469616C423A70617373776F7264' }, BatchOrderOption='true', BatchErrorContinuationOption='Continue'

In: uuidKey

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Authentication (0x42000C), Type: Structure (0x01), Data:
      Tag: Credential (0x420023), Type: Structure (0x01), Data:
        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001
        Tag: Credential Value (0x420025), Type: Octet String (0x08), Data:
43726564656E7469616C423A70617373776F7264
    Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE
    Tag: Batch Error Continuation Option (0x42000E), Type: Enumeration (0x05), Data: 0x00000001
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: B759AEB1E797807E
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 81d1d04a-e47f-40ec-a48f-
1fca748b976a
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7E8684670DAD2857
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 81d1d04a-e47f-40ec-a48f-
1fca748b976a
```

```
42007801000001604200770100000098420069010000002042006A02000000040000000100000000042006B02000000040
000000000000000042000C01000000384200230100000030420024050000000400000001000000004200250800000001443
726564656E7469616C423A70617373776F72640000000004200100600000008000000000000000142000E0500000004000
00001000000000042000D0200000004000000020000000042000F01000000584200 5C050000000400000000A000000004200
930800000008B759AEB1E797807E4200790100000030420094070000002434373435353138622D633466312D343362312
D383035302D36376462663738393235633200000000042000F01000000584200 5C050000000400000000C00000000420093
08000000087E8684670DAD285742007901000000304200940700000024343734353531386 22D633466312D343362312D3
83035302D36376462663738393235633200000000
```

Out: Operation Failed, Permission Denied

Out: Operation Failed, Permission Denied

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B757911 (Fri Feb 12
16:51:45 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: B759AEB1E797807E
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)
    Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x0000000C (Permission Denied)
    Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Access denied
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
    Tag: Unique Batch Item ID (0x420093), Type: Octet String (0x08), Data: 7E8684670DAD2857
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)
    Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x0000000C (Permission Denied)
    Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Access denied
```

```
42007B01000001104200 7A0100000048420069010000002042006A02000000040000000100000000042006B02000000040
0000000000000004200920900000008000000004B7579114200 0D0200000004000000020000000042000F010000005842
005C0500000004000000A000000004200930800000008B759AEB1E797807E42007F050000000400000001000000000420
07E0500000004000000C000000004200 7D070000000D4163636573732064656E696564000000042000F0100000058420 0
5C0500000004000000C000000004200930800000087E8684670DAD285742007F05000000040000000100000000042007
E0500000004000000C000000004200 7D070000000D4163636573732064656E696564000000
```

3

Destroy

In (header): credential={ credentialType='1', credentialValue="0x43726564656E7469616C413A736563726574' }

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Authentication (0x42000C), Type: Structure (0x01), Data:
      Tag: Credential (0x420023), Type: Structure (0x01), Data:
        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001
        Tag: Credential Value (0x420025), Type: Octet String (0x08), Data: 
43726564656E7469616C413A736563726574
    Tag: 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: 81d1d04a-e47f-40ec-a48f-
1fca748b976a

42007801000000D04200770100000078420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000042000C0100000038420023010000003042002405000000040000000100000000420025080000001243
726564656E7469616C413A736563726574000000000000042000D0200000004000000010000000042000F0100000048420
05C0500000004000000140000000042007901000000304200940700000024383164316430346120653437662D34306563
2D613438662D3166636137343862393736610000000
```

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: 0x000000004B757912 (Fri Feb 12 
16:51:46 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 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: 81d1d04a-e47f-40ec-a48f-
1fca748b976a

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
0000000000000004200920900000008000000004B75791242000D0200000004000000010000000042000F010000005842
005C0500000004000000140000000042007F0500000004000000000000000042007C010000003042009407000000024383
164316430346120653437662D343065632D613438662D3166636137343862393736610000000
```

4 Get Attributes

In (header): credential={ credentialType='1', credentialValue=''0x43726564656E7469616C413A736563726574' }

In: uuidKey, attributeNames={ 'Destroy Date' }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Authentication (0x42000C), Type: Structure (0x01), Data:
      Tag: Credential (0x420023), Type: Structure (0x01), Data:
        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001
        Tag: Credential Value (0x420025), Type: Octet String (0x08), Data:
```

```
43726564656E7469616C413A736563726574
    Tag: 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: 81d1d04a-e47f-40ec-a48f-
1fca748b976a
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Destroy Date

42007801000000E84200770100000078420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042000C0100000038420023010000003042002405000000040000000100000000420025080000001243
726564656E7469616C413A7365637265740000000000000042000D0200000004000000010000000042000F0100000060420
05C0500000004000000B000000004200790100000048420094070000002438316431643034612D653437662D34306563
2D613438662D3166636137343862393736610000000042000A070000000C44657374726F79204461746500000000
```

Out: uuidKey, attributes={ DestroyDate=' 0x000000004B757912' }

```
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: 0x000000004B757912 (Fri Feb 12
16:51:46 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 81d1d04a-e47f-40ec-a48f-
1fca748b976a
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Destroy Date
        Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data: 0x000000004B757912 (Fri
Feb 12 16:51:46 CET 2010)

42007B01000000E042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420092090000000800000004B75791242000D0200000004000000010000000042000F010000008842
005C0500000004000000B000000042007F0500000004000000000000000042007C010000006042009407000000024383
164316430346120653437662D343065632D613438662D3166636137343862393736610000000042000801000000284200
0A070000000C44657374726F792044617465000000042000B09000000080000000004B757912
```

12 Query, Maximum Response Size

Formatted: Bullets and Numbering

This use case tests the Query operation and the Maximum Response Size header field.

12.1 Use-case: Query, Maximum Response Size

Formatted: Bullets and Numbering

Perform a Query operation, querying the Operations and Objects supported by the server, with a restriction on the Maximum Response Size set in the request header. Since the resulting Query response is too big, an error is returned. Increase the Maximum Response Size, resubmit the Query request, and get a successful response.

Time	Request/Response

0	Query (operations, objects)
	In (header): maximumResponseSize='256'
	In: queryFunctions={ '00000001', '00000002' }
	
	`Tag: Request Message (0x420078), Type: Structure (0x01), Data:`
	`  Tag: Request Header (0x420077), Type: Structure (0x01), Data:`
	`    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)`
	`    Tag: Maximum Response Size (0x420050), Type: Integer (0x02), Data: 0x00000100 (256)`
	`    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:`
	`    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000018 (Query)`
	`    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:`
	`      Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000001 (Operations)`
	`      Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000002 (Objects)`
	
	`42007801000000904200770100000048420069010000002042006A0200000004000000010000000042006B02000000040`
	`000000000000000420050020000000400000100000000042000D0200000004000000010000000042000F010000003842`
	`005C050000000400000018000000004200790100000020420074050000000400000001000000004200740500000004000`
	`0000200000000`
	
	Out: Operation Failed, Response Too Large
	
	`Tag: Response Message (0x42007B), Type: Structure (0x01), Data:`
	`  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:`
	`    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)`
	`    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B7918AA (Mon Feb 15 10:49:30 CET 2010)`
	`    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)`
	`    Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x00000002 (Response Too Large)`
	`    Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Response size: 568, Maximum Response Size indicated in request: 256`
	`    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000000 (0)`
	
	`42007B01000000C042007A01000000B8420069010000002042006A0200000004000000010000000042006B02000000040`
	`00000000000000042009209000000080000000004B7918AA42007F0500000004000000010000000042007E050000000400`
	`0000020000000042007D07000000435265737706F6E73652073697A653A203536382C204D6178696D756D20526573706F6`
	`E73652053697A6520696E64696361746564420696E2072657175657374 3A2032353600000000000042000D020000000400000`
	`000000000000`

1	Query (operations, objects) In (header): maximumResponseSize='2048'

In: queryFunctions={ ‘00000001’, ‘00000002’ }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Maximum Response Size (0x420050), Type: Integer (0x02), Data: 0x00000800 (2048)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000018 (Query)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000001 (Operations)
      Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000002 (Objects)
```

```
42007801000000904200770100000048420069010000002042006A0200000004000000010000000042006B02000000040
000000000000000420050020000000400000800000000004200D0D020000000400000001000000000042000F010000003842
005C05000000040000001800000000420079010000002042007405000000040000000100000000420074050000000400 0
00000200000000
```

Out: operations, objects

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004B7918AA (Mon Feb 15
10:49:30 CET 2010)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000018 (Query)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000002 (Create Key Pair)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000004 (Re-key)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000008 (Locate)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000009 (Check)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000B (Get Attributes)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000C (Get Attribute List)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000D (Add Attribute)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000E (Modify Attribute)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000010 (Obtain Lease)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage
Allocation)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000012 (Activate)
```

```
        Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
        Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 (Destroy)
        Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000015 (Archive)
        Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000016 (Recover)
        Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000018 (Query)
        Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000019 (Cancel)
        Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001A (Poll)
        Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000001 (Certificate)
        Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002 (Symmetric Key)
        Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000003 (Public Key)
        Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000004 (Private Key)
        Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000006 (Template)
```

42007B010000023042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040
00000000000000042009209000000080000000004B7918AA42000D0200000004000000010000000042000F01000001D842
005C05000000040000001800000000042007F0500000004000000000000000042007C01000001B042005C0500000004000
00001000000000042005C050000000400000002000000000042005C050000000400000003000000000042005C05000000040000
00040000000042005C050000000400000008000000000042005C050000000400000009000000000042005C0500000004000000
00A0000000042005C05000000040000000B0000000042005C05000000040000000C0000000042005C050000000400000000
0D0000000042005C05000000040000000E0000000042005C05000000040000000F0000000042005C05000000040000001
00000000042005C050000000400000011000000000042005C050000000400000012000000000042005C050000000400000013
0000000042005C050000000400000014000000000042005C050000000400000015000000000042005C050000000400000160
00000000042005C050000000400000018000000000042005C050000000400000019000000000042005C05000000040000001A00
000000420057050000000400000001000000004200570500000004000000020000000042005705000000040000000003000
000004200570500000004000000040000000042005705000000040000000600000000

303

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

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

B. Revision History

Revision	Date	Editor	Changes Made
ed-0.98	2009-04-28	Mathias Björkqvist	Initial conversion of input document to OASIS format.
ed-0.98	2009-08-06	Mathias Björkqvist	Changes to layout and message content to reflect the recent changes to the KMIP specification, added descriptions to the use-cases for which they were missing.
ed-0.98	2009-09-28	Mathias Björkqvist	Updated messages and TTLV encodings to conform with KMIP specification ed-0.98 rev 17.
draft-01	2009-10-08	Mathias Björkqvist	Removed normative words “must”, “shall”, “required”, “will” and “can”; updated messages and TTLV encodings to conform to KMIP specification ed-0.98 rev 19; added normative references; added minor edits
draft-02	2009-10-15	Mathias Björkqvist	Replaced the TBDs, changed status to Committee Draft, changed use-cases to use protocol major version 1 and minor version 0
draft-03	2009-10-15	Mathias Björkqvist	Corrected names of TC chairs
draft-04	2009-11-05	Mathias Björkqvist	Added list of participants, added reference to Profiles document, line spacing change to list of original contributors, added related documents
cd-05	2009-11-06	Mathias Björkqvist	Changes to various naming aspects on front page and document footer. This is the tentative version for public review.
cd-06	2009-11-12	Mathias Björkqvist	Updated tags.
cd-07	2010-02-17	Mathias Björkqvist	Addressed public review comments, added line numbering.

Deleted: ¶

Page 48: [1] Deleted **Mathias Björkqvist** **2/17/2010 2:40 PM**

```
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)

42007801000000C042007701000000384200690100000020420006A0200000004000000010000000042006B020
000000400000000000000000042000D0200000004000000010000000042000F010000007842005C050000000400
00000D0000000042007901000000604200940700000024323164323862386 12D303664662D343363302D62373
2662D326131363136333361646139000000004200080100000028420000A070000000F41637469766174696F6E
20446174650042000B09000000080000000000000002
```

Page 49: [2] Deleted **Mathias Björkqvist** **2/17/2010 2:40 PM**

```
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-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)

42007B01000000E042007A0100000048420069010000002042006A0200000004000000010000000042006B020
00000040000000000000000042009209000000080000000004AFBED2B42000D02000000040000000100000000042
000F010000008842005C05000000040000000D0000000042007F0500000004000000000000000042007C01000
000604200940700000024323164323862386 12D303664662D343363302D623732662D32613136313633336164
6139000000004200080100000028420000A070000000F41637469766174696F6E20446174650042000B0900000
0080000000000000002
```