This is a Non-Standards Track Work Product. The patent provisions of the OASIS IPR Policy do not apply.

Key Management Interoperability Protocol Test Cases Version 1.1

Committee Note 01

27 July 2012

Specification URIs

This version:

http://docs.oasis-open.org/kmip/testcases/v1.1/cn01/kmip-testcases-v1.1-cn01.doc (Authoritative)
http://docs.oasis-open.org/kmip/testcases/v1.1/cn01/kmip-testcases-v1.1-cn01.html
http://docs.oasis-open.org/kmip/testcases/v1.1/cn01/kmip-testcases-v1.1-cn01.pdf

Previous version:

http://www.oasis-open.org/committees/download.php/44882/kmip-usecases-v1.1-cnprd01.zip

Latest version:

http://docs.oasis-open.org/kmip/testcases/v1.1/kmip-testcases-v1.1.doc (Authoritative)
http://docs.oasis-open.org/kmip/testcases/v1.1/kmip-testcases-v1.1.html
http://docs.oasis-open.org/kmip/testcases/v1.1/kmip-testcases-v1.1.pdf

Technical Committee:

OASIS Key Management Interoperability Protocol (KMIP) TC

Chairs:

Robert Griffin (robert.griffin@rsa.com), EMC Corporation
Subhash Sankuratripati (Subhash.Sankuratripati@netapp.com), NetApp

Editors:

Mathias Björkqvist (mbj@zurich.ibm.com), IBM
Tim Hudson (tjh@cryptsoft.com), Cryptsoft

Related work:

This document replaces or supersedes:

- *Key Management Interoperability Protocol Use Cases Version 1.0*. Committee Specification 01. 15 June 2010. http://docs.oasis-open.org/kmip/usecases/v1.0/cs01/kmip-usecases-1.0-cs-01.html.

This document was previously published as:

- *Key Management Interoperability Protocol Use Cases Version 1.1.* 04 January 2012. Committee Note Draft 01 / Public Review Draft 01. http://www.oasis-open.org/committees/download.php/44882/kmip-usecases-v1.1-cnprd01.zip

This document is related to:

- *Key Management Interoperability Protocol Specification Version 1.1*. Latest version. http://docs.oasis-open.org/kmip/spec/v1.1/kmip-spec-v1.1.html
- *Key Management Interoperability Protocol Profiles Version 1.1*. Latest version. http://docs.oasis-open.org/kmip/profiles/v1.1/kmip-profiles-v1.1.html
- Key Management Interoperability Protocol Usage Guide Version 1.1. Latest version. http://docs.oasis-open.org/kmip/ug/v1.1/kmip-ug-v1.1.html

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 OASIS Key Management Interoperability Protocol (KMIP) TC on the above date. The level of approval is also listed above. Check the “Latest version” location noted above for possible later revisions of this document.

Technical Committee members should send comments on this document 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/.

Citation format:

When referencing this document the following citation format should be used:

[KMIP-TC]

Key Management Interoperability Protocol Test Cases Version 1.1. 27 July 2012. OASIS Committee Note 01. http://docs.oasis-open.org/kmip/testcases/v1.1/cn01/kmip-testcases-v1.1-cn01.html

Table of Contents

1 Introduction

The purpose of this document is to describe test cases to demonstrate the Key Management Interoperability Protocol (KMIP) [KMIP-Spec]

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof]. The test cases indicate if all concepts within the protocol are sound and if the protocol is usable when implementing typical scenarios in real life. These test cases are not intended to fully test an implementation of KMIP. Thus, the test cases do not contain typical Quality Assurance scenarios which would stress an implementation. The test cases are based on v1.0 of the protocol.

The test 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 test 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 test 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 test 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]

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof]). 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 test 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-Spec]

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[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 References

[KMIP-Spec]
Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof]
Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/profiles/v1.1/cd01/kmip-profiles-1.1-cd-01.doc

[KMIP-UG]
Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/ug/v1.1/cd01/kmip-ug-1.1-cd-01.doc

[NISTKeyWrap]
AES Key Wrap Specification. November 2001. NIST.
http://csrc.nist.gov/groups/ST/toolkit/documents/kms/key-wrap.pdf

2 Message Exchange

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

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof] and [KMIP-Spec]

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof].

3 Centralized Management

3.1 Basic Functionality

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

3.1.1 Test Case: Create / Destroy

In this test 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: 0x00000001 (1)
	    Tag: 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)
```

```
42007801000001204200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000D84200
5C0500000004000000010000000042007901000000C042005705000000040000000200000000420091
01000000A84200080100000030420000A070000001743727970746F677261706869632041 6C676F7269
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E5
(Fri Apr 27 10:12:21 CEST 2012)

    Tag: 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: fb4b5b9c-
6188-4c63-8142-fe9c328129fc
```

```
42007B01000000C042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A54E542000D0200000004000
0000100000000042000F010000006842005C0500000004000000010000000042007F05000000040000000
00000000042007C0100000040420057050000000400000002000000004200940700000024666234622
356239632D363138382D346336332D383134322D6665396333323831323966630000000
```

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:
0x00000001 (1)
    Tag: 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: fb4b5b9c-
6188-4c63-8142-fe9c328129fc
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C050000000400000014000000004200790100000030420094070000002466623462356239632D3631
38382D346336332D383134322D6665396333323831323966630000000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E5 
(Fri Apr 27 10:12:21 CEST 2012)

    Tag: 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: fb4b5b9c-
6188-4c63-8142-fe9c328129fc



42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B020000000400000001000000004200920900000008000000004F9A54E542000D02000000040000
0001000000000042000F01000000584200 5C0500000004000000140000000042007F0500000004000000
00000000042007C0100000030420094070000002466623462356239632D363138382D346336332D38
3134322D666539633332383132396663000000000
```

3.1.2 Test Case: Register / Create / Get attributes / Destroy

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

Time	Request/Response messages

0	Register (template)
	In: objectType='00000007', TemplateAttribute=empty, Template={ ObjectGroup='Group1', ApplicationSpecificInformation='ssl, www.example.com', ContactInformation='Joe', x-Purpose='demonstration', Name={ NameValue='Template1', NameType='00000001' } }
	`Tag: Request Message (0x420078), Type: Structure (0x01), Data:`

```
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
    Tag: 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: null
      Tag: Template (0x420090), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Group
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Group1
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Application Specific Information
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Application Namespace (0x420003), Type: Text String (0x07), Data: ssl
            Tag: Application Data (0x420002), Type: Text String (0x07), Data: www.example.com
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Contact Information
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: Joe
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-Purpose
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: demonstration
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: Template1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001
```

```
(Uninterpreted Text String)
```

```
42007801000001C84200770100000038420069010000002042006A02000000040000000100000000420
06B02000000040000000100000000042000D02000000040000000100000000042000F01000001804200
5C0500000004000000030000000042007901000001684200570500000004000000060000000042009101
00000000420090010000014842000801000000284200A070000000C4F626A6563742047726F7570
000000042000B07000000647726F75703100004200080100000058420000A070000000204170706C69
636174696F6E20537065636966696320496E666F726D6174696F6E42000B010000002842000307000
0000373736C00000000004200020700000000F7777772E6578616D706C652E636F6D00420008010000000
3042000A07000000013436F6E7461637420496E666F726D6174696F6E000000000042000B0700000003
4A6F650000000000004200080100000003042000A0700000009782D507572706F73650000000000000042
000B070000000D64656D6F6E7374726174696F6E0000004200080100000004042000A07000000044E61
6D650000000042000B010000002842005507000000954656D706C617465310000000000000420054
05000000040000000100000000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E5
(Fri Apr 27 10:12:21 CEST 2012)
    Tag: 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: 5c9b81ef-
4ee5-42cd-ba2d-c002fdd0c7b3
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B020000000400000001000000004200920900000008000000004F9A54E542000D020000000400000
00010000000042000F01000000584200005C050000000400000003000000000042007F0500000004000000
000000000042007C010000003042009407000000243563396238316566662D346565352D343263642D62
6132642D633030326664643063376233300000000
```

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: 0x00000001 (1)
    Tag: 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)

        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)
```

```
4200780100000190420077010000003842006901000000204200 6A02000000040000000100000000 42
```

```
42007801000001904200770100000038420069010000002042006A020000000400000001000000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000001484200
5C0500000004000000010000000042007901000001304200570500000004000000020000000000420091
0100000118420053010000002842005507000000095465 6D706C617465310000000000000000420054 05
0000000400000001000000004200080100000030 42000A070000001743727970746F67726170686963
20416C676F726974686D0042000B05000000040000000300000000420008010000003042000A070000
00144372797074 6F67726170686963204C656E6774680000000042000B02000000040000008000000 0
004200080100000030 42000A070000001843727970746F677261706869632055736167 65204D61736B
42000B02000000040000000C00000000420008010000003842000A07000000044E616D650000000042
000B01000000204200550700000004 4B657931000000004200540500000004000000010 0000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E6
(Fri Apr 27 10:12:22 CEST 2012)

    Tag: 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: 1703250b-
4d40-4de2-93a0-c494a1d4ae40
```

	42007B01000000C042007A0100000048420069010000002042006A02000000040000000100000000420 06B02000000040000000100000000420092090000000800000004F9A54E642000D020000000400000 0010000000042000F010000006842005C050000000400000001000000042007F050000000400000000 0000000042007C0100000040420057050000000400000002000000004200940700000024313730333 23530622D346434302D346465322D393361302D63343934613164346165343000000000
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: 0x00000001 (1) Tag: 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: 1703250b-4d40-4de2-93a0-c494a1d4ae40 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 42007801000001084200770100000038420069010000002042006A02000000040000000100000000420 06B02000000040000000100000000420000D02000000040000000100000000420000F01000000C04200 5C0500000004000000B00000000420079010000000A84200940700000024313730333235306220D3464 34302D346465322D393361302D63343934613164346165343000000000042000A070000000C4F626A65 63742047726F7570000000000042000A0700000020417070C69636174696F6E2053706563696669632 0 496E666F726D6174696F6E42000A070000013436F6E7461637420496E666F726D6174696F6E000000 000042000A0700000009782D507572706F7365000000000000000

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E6
(Fri Apr 27 10:12:22 CEST 2012)
    Tag: 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: 1703250b-
4d40-4de2-93a0-c494a1d4ae40
      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
```

```
42007B01000001B042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000000400000001000000004200920900000008000000004F9A54E642000D02000000040000
0001000000000042000F010000015842005C0500000004000000000B0000000042007F0500000004000000
00000000000042007C010000013042009407000000243137303332353062 2D346434302D346465322D39
3361302D63343934613164346165343000000000042000801000000284 2000A070000000C4F626A6563
742047726F75700000000000042000B070000000647726F75703100004200080100000058 42000A070000
00204170706C69636174696F6E205370656369666963320496E666F726D6174696F6E42000B01000000
28420003070000000373736C000000000004200020700000000F7777772E6578616D706C652E636F6D00
42000801000000304 2000A070000001343 6F6E7461637420496E666F726D6174696F6E000000000042
000B07000000034A6F650000000000004200080100000030 42000A0700000009782D507572706F736500
0000000000042000B070000000D64656D6F6E7374726174696F6E000000
```

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:
0x00000001 (1)

    Tag: 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: 1703250b-
4d40-4de2-93a0-c494a1d4ae40
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B0200000000400000001000000004200 0D0200000004000000010000000042000F01000000484200
5C05000000040000001400000000420079010000003042009407000000243137303332353062 2D3464
34302D346465322D393361302D633439346131643461653430000000000
```

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: 0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E6 (Fri Apr 27 10:12:22 CEST 2012) Tag: 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: 1703250b-4d40-4de2-93a0-c494a1d4ae40 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042 006B0200000004000000010000000042009209000000080000000004F9A54E642000D0200000004000000 00010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000 0000000000042007C0100000030420094070000002431373033323530622D346434302D346465322D39 3361302D633439346131643461653430000000000
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: 0x00000001 (1)

```
    Tag: 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: 5c9b81ef-
4ee5-42cd-ba2d-c002fdd0c7b3
```

```
420078010000009042007701000000384200690100000020420006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000484200
5C05000000040000001400000000420079010000003042009407000000243563396238316566 2D3465
65352D343263642D626132642D63303032666464306337623300000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E6
(Fri Apr 27 10:12:22 CEST 2012)

    Tag: 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: 5c9b81ef-
4ee5-42cd-ba2d-c002fdd0c7b3
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B020000000400000001000000004200920900000008000000004F9A54E642000D0200000004000000
0001000000000042000F010000005842005C0500000004000000140000000042007F0500000004000000
00000000000042007C01000000304200940700000024356339623831656662D346565352D343263642D62
6132642D63303032666464306337623300000000
```

3.1.3 Test Case: Create / Locate / Get / Destroy

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

Time	Request/Response messages

0	Create (symmetric key)
	In: objectType = ‘00000002’, attributes={ Name={ NameValue=‘Key1’, NameType=’00000001’ }, CryptographicAlgorithm=’3DES’, CryptographicLength=’168’, 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: 0x00000001 (1)
	    Tag: 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



42007801000001984200770100000038420069010000002042006A02000000040000000100000000420
06B0200000004000000010000000042000D0200000004000000010000000042000F01000001504200
5C0500000004000000010000000042007901000001384200570500000004000000020000000042009 1
0100000120420008010000003842000A07000000044E616D650000000042000B010000002042005507
000000044B6579310000000042005405000000040000000100000000420008010000003042000A0700
0000174372797074 6F67726170686963 20416C676F726974686D0042000B0500000004000000020000
00004200080100000030 42000A070000001443727970746F67726170686963204C656E677468000000
0042000B02000000040000 00A80000000042000801000000 3042000A070000001843727970746F6772
6170686963205573616765204D61736B42000B02000000040000000C00000000420008010000003042
000A0700000013436F6E7461637420496E666F726D6174696F6E000000000042000B07000000034A6F
650000000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E6
(Fri Apr 27 10:12:22 CEST 2012)
```

	Tag: 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: 49a1ca88-6bea-4fb2-b450-7e58802c3038 42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042 006B02000000040000000100000000420092090000000800000004F9A54E642000D020000000400000 0001000000000042000F010000006842005C0500000004000000010000000042007F050000000400000 00000000000042007C0100000040420057050000000400000002000000004200940700000024343961 31 636138382D366265612D346662322D623435302D37653538383032633330333800000000
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: 0x00000001 (1) Tag: 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)
```

```
42007801000000D042007701000000384200690100000020420006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000884200
5C0500000004000000080000000042007901000000704200080100000028420000A070000000B4F626A
656374205479706500000000042000B0500000004000000020000000042000801000000384200A07
000000044E616D6500000000042000B010000002042005507000000044B657931000000004200540500
0000040000000100000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E6
(Fri Apr 27 10:12:22 CEST 2012)

    Tag: 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: 49a1ca88-
6bea-4fb2-b450-7e58802c3038
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042009209000000080000000004F9A54E642000D02000000040000
00010000000042000F01000000058420055C0500000004000000080000000042007F0500000004000000
00000000000042007C010000003042009407000000024343961316361383822D366265612D346662322D62
3435302D3765353838303263333033380000000
```

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: 
0x00000001 (1)
    Tag: 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: 49a1ca88-
6bea-4fb2-b450-7e58802c3038
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C0500000004000000A0000000042007901000000304200940700000024343961316361383 82D3662
65612D346662322D623435302D37653538383032633330333800000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E7 
(Fri Apr 27 10:12:23 CEST 2012)
    Tag: 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: 49a1ca88-6bea-4fb2-b450-7e58802c3038 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 (Raw) Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 7367578051012A6D134A855E25C8CD5E4CA131455729D3C8 Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000002 (3DES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x000000A8 (168) 42007B010000012842007A0100000048420069010000002042006A0200000004000000010000000042 006B020000000400000001000000004200920900000008000000004F9A54E742000D0200000004000000 0001000000000042000F01000000D042005C0500000004000000A0000000042007F0500000004000000 0000000000042007C01000000A84200570500000004000000020000000042009407000000243439613 1 636138382D366265612D346662322D623435302D3765353838303263333033380000000042008F0100 0000604200400100000058420042050000000400000001000000004200450100000020420043080000 00187367578051012A6D134A855E25C8CD5E4CA131455729D3C8420028050000000400000002000000 0042002A0200000004000000A800000000
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: 0x00000001 (1) Tag: 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: 49a1ca88-6bea-4fb2-b450-7e58802c3038
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000420
06B02000000040000000100000000420000D020000000400000001000000000420000F01000000484200
5C0500000004000000140000000042007901000000304200940700000024343961316361383 82D3662
65612D346662322D623435302D37653538383032633330333800000000
```

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: 0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E7 (Fri Apr 27 10:12:23 CEST 2012)
    Tag: 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: 49a1ca88-6bea-4fb2-b450-7e58802c3038
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420
06B020000000400000001000000004200920900000008000000004F9A54E742000D0200000004000
00001000000000042000F01000000584200 5C050000000400000014000000004200 7F0500000004000000
00000000000042007C010000003042009407000000243439613163613838 2D366265612D346662322D62
3435302D37653538383032633330333800000000
```

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: 
0x00000001 (1)
    Tag: 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: 49a1ca88-
6bea-4fb2-b450-7e58802c3038
```

```
42007801000000B84200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000704200
5C050000000400000008000000004200790100000058420008010000005042000A0700000011556E69
717565204964656E7469666965720000000000000042000B070000002434396131636138382D366265
612D346662322D623435302D37653538383032633330333800000000
```

Out: <empty response payload>

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E7
```

	(Fri Apr 27 10:12:23 CEST 2012)
	    Tag: 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
	
	42007B010000008042007A0100000048420069010000002042006A0200000004000000010000000042
	006B02000000040000000100000000420092090000000800000000 4F9A54E742000D02000000040000
	00010000000042000F010000002842005C05000000040000000800000000 42007F0500000004000000
	000000000042007C0100000000

3.1.4 Test Case: Dual Client Test Case, ID Placeholder-linked Locate & Get Batch

This test 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 test 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.

Time	Request/Response messages
0	Client A: Register (template) In: objectType='00000007', TemplateAttribute=empty, Template={ 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:
0x00000001 (1)
    Tag: 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: null
      Tag: Template (0x420090), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data:
Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data:
0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data:
Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080
(128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: Template1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001
(Uninterpreted Text String)
```

```
42007801000001384200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000F04200
5C05000000040000000300000000420079010000000D842005705000000040000000600000000420091
0100000000420090010000000B842000801000000003042000A070000000174372797074 6F677261706869
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E7 
(Fri Apr 27 10:12:23 CEST 2012)
    Tag: 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: d83a3a7e-
62a3-4f2b-bfe7-11544759000d
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A54E742000D0200000004000000
00010000000042000F01000000584200 5C0500000004000000030000000042007F0500000004000000
000000000042007C010000003042009407000000246438336133613765 2D363261332D346632622D62
6665372D313135343437353930303064 00000000
```

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: 
```

```
0x00000001 (1)
    Tag: 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
```

```
42007801000001584200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000001104200
5C050000000400000001000000004200790100000F8420057050000000400000002000000000420091
01000000E04200530100000028420055070000000954656D706C6174653100000000000000042005405
000000040000000100000000420008010000003842000A07000000044E616D6500000000042000B0100
0000204200550700000044B65793100000000420054050000000400000001000000004200080100000
003042000A070000001843727970746F677261706869632055736167652044D61736B42000B02000000
0400000004000000004200080100000003042000A0700000013436F6E746163742049 6E666F726D6174
696F6E000000000042000B0700000003466F6F0000000000
```

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: 0x00000001 (1)
	    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E7 (Fri Apr 27 10:12:23 CEST 2012)
	    Tag: 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: b4faee10-aa2a-4446-8ad4-0881f3422959
	
	42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042
	006B020000000400000001000000004200920900000008000000004F9A54E742000D02000000040000
	00010000000042000F010000006842005C0500000004000000010000000042007F0500000004000000
	000000000042007C010000004042005705000000040000000200000000420094070000002462346661
	656531302D616132612D343434362D386164342D30383831663334323239353900000000

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: 
0x00000001 (1)

    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: Byte String (0x08), Data: 
AA21F8C659D6E10D

    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: Byte String (0x08), Data: 
495A95F165854D1E

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

```
42007801000001204200770100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420010060000000800000000000000014200D020000000040000
00020000000042000F01000000984200 5C05000000040000000800000000420093080000000 8AA21F8
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E7 
(Fri Apr 27 10:12:23 CEST 2012)
    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: Byte String (0x08), Data: 
AA21F8C659D6E10D
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 
(Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b4faee10-
aa2a-4446-8ad4-0881f3422959
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
495A95F165854D1E
    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: b4faee10-
aa2a-4446-8ad4-0881f3422959
      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 (Raw)
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 
D351910F1D7934D6E2AE17576564E2BC
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 
0x00000003 (AES)
```

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

```
42007B01000001A042007A0100000048420069010000002042006A02000000040000000100000000420
06B0200000004000000010000000042009209000000080000000004F9A54E742000D02000000040000
0002000000000042000F010000006842005C0500000004000000080000000042009308000000008AA21F8
C659D6E10D42007F0500000004000000000000000042007C010000003042009407000000246234666
1656531302D616132612D343434362D386164342D303838316633343232393539000000000042000F0100
0000D842005C0500000004000000A0000000042009308000000008495A95F165854D1E42007F050000
00040000000000000000042007C01000000A042005705000000040000000200000000420094070000000
24623466616565313024D616132612D343434362D386164342D30383831663334323239353900000000
42008F01000000584200400100000050420042050000000400000001000000004200450100000018420
0430800000010D351910F1D7934D6E2AE17576564E2BC420028050000000400000003000000004200
2A020000000400000080000000000
```

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: 
0x00000001 (1)
    Tag: 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: b4faee10-
aa2a-4446-8ad4-0881f3422959
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000420
06B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000000C0000000042007901000000304200940700000024623466616565313302D6161
32612D343434362D386164342D303838316633343232393539000000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E7
(Fri Apr 27 10:12:23 CEST 2012)

    Tag: 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: b4faee10-
aa2a-4446-8ad4-0881f3422959

      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: Lease Time

      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
```

```
42007B01000001E042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000000004F9A54E742000D02000000040000
00010000000042000F010000018842005C05000000040000000C0000000042007F0500000004000000
000000000042007C010000016042009407000000246234666165653130 2D616132612D343434362D38
6164342D303838316633343232393539000000042000A070000001443727970746F677261706869 63
204C656E67746800000000 42000A07000000174372797074 6F67726170686963 20416C676F72697468
6D0042000A0700000005537461746500000042000A070000000644696765737400 0042000A07000000
0A4C656173652054696D65000000000000 42000A070000000C496E697469616C204461746500000000
42000A0700000011556E69717565204964656E746966696572000000000000000042000A07000000044E
616D650000000042000A070000001843727970746F67726170686963205573616765204D61736B4200
0A070000000B4F626A6563742054797065000000000042000A0700000013436F6E7461637420496E66
6F726D6174696F6E000000000042000A07000000104C617374204368616E67652044617465
```

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: 
0x00000001 (1)

    Tag: 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: b4faee10-
aa2a-4446-8ad4-0881f3422959

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

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

```
42007801000000C04200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F0100000078 4200
5C05000000040000000B000000004200790100000060420094070000002462346661656531302D6161
32612D343434362D386164342D30383831663334323239353900000000 42000A07000000044E616D65
0000000042000A0700000013436F6E7461637420496E666F726D6174696F6E0000000000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E7
(Fri Apr 27 10:12:23 CEST 2012)
    Tag: 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: b4faee10-
aa2a-4446-8ad4-0881f3422959
      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
```

```
42007B010000012842007A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A54E742000D02000000040000
000100000000042000F01000000D042005C05000000040000000B0000000042007F0500000004000000
000000000042007C01000000A8420094070000002462346661656531302D616132612D343434362D38
6164342D30383831663334323239353900000000420008010000003842000A07000000044E616D6500
00000042000B010000002042005507000000044B657931000000004200540500000004000000010000
0000420008010000003042000A0700000013436F6E7461637420496E666F726D6174696F6E00000000
0042000B0700000003466F6F0000000000
```

5

Client B:

Add attribute [batch]

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

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

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
    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: Byte String (0x08), Data: 32D84369C120488E
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b4faee10-aa2a-4446-8ad4-0881f3422959
      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: Byte String (0x08), Data: 519CF4F0EC1AC13F
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b4faee10-aa2a-4446-8ad4-0881f3422959
      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
```

```
42007801000001604200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000020000000042000F01000000884200
5C05000000040000000D00000000420093080000000832D84369C120488E42007901000000604200940
700000024623466616565313 02D616132612D343434362D386164342D303838316633343232393539
000000004200080100000028 42000A070000000C782D6174747269627574653100000000 42000B0700
00000656616C756531000042000F01000000884200 5C05000000040000000D00000000420093080000
0008519CF4F0EC1AC13F4200790100000060420094070000002462346661656531302D616132612D34
3434362D386164342D30383831663334323239353900000000420008010000002842000A070000000C
782D6174747269627574653200000000 42000B070000000656616C7565320000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E7
(Fri Apr 27 10:12:23 CEST 2012)

    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: Byte String (0x08), Data:
32D84369C120488E

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b4faee10-
aa2a-4446-8ad4-0881f3422959

      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: Byte String (0x08), Data: 
519CF4F0EC1AC13F

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b4faee10-
aa2a-4446-8ad4-0881f3422959

      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



42007B010000019042007A01000000484200690100000020420069A020000000400000001000000000042
```

```
42007B010000019042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A54E742000D020000000400000
0002000000000042000F010000009842005C050000000400000000D00000000420093080000000832D843
69C120488E42007F0500000004000000000000000042007C010000006042009407000000002462346661
656531302D616132612D343434362D386164342D303838316633343232393539000000004200080100
00002842000A070000000C782D617474726962757465310000000042000B070000000656616C756531
000042000F010000009842005C05000000040000000D00000000420093080000000008519CF4F0EC1AC1
3F42007F0500000004000000000000000042007C01000000604200940700000024623466616565313
2D616132612D343434362D386164342D3038383166333432323935390000000042000801000000284
000A070000000C782D617474726962757465320000000042000B070000000656616C7565320000
```

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: 
0x00000001 (1)

    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: Byte String (0x08), Data: FCE08E45995686B6

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b4faee10-aa2a-4446-8ad4-0881f3422959

      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: Byte String (0x08), Data: DC2BFDA88F39F5FC

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b4faee10-aa2a-4446-8ad4-0881f3422959

      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
```

```
42007801000001704200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000020000000042000F01000000904200
5C0500000004000000E0000000042009308000000008FCE08E45995686B64200790100000068420094
07000000246234666165653130 2D616132612D343434362D386164342D303838316633343232393539
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E7
(Fri Apr 27 10:12:23 CEST 2012)
    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: Byte String (0x08), Data:
FCE08E45995686B6
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000
(Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b4faee10-
aa2a-4446-8ad4-0881f3422959
      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: Byte String (0x08), Data:
DC2BFDA88F39F5FC
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000
(Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b4faee10-
aa2a-4446-8ad4-0881f3422959
      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
```

```
42007B01000001A042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A54E742000D02000000040000
0002000000042000F01000000A042005C0500000004000000E00000000420093080000008FCE08E
45995686B642007F0500000004000000000000000042007C01000000684200940700000002462346661
```

	656531302D616132612D343434362D386164342D30383831663334323239353900000000420008 0100 00003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F64696669 656456616C756531000042000F01000000A042005C05000000040000000E0000000042009308000000 08DC2BFDA88F39F5FC42007F0500000004000000000000000042007C0100000068420094070000002 4 62346661656531302D616132612D343434362D386164342D3038383166333432323935390000000042 000801000000003042000A070000000C782D617474726962757465320000000042000B070000000E4D6F 646966696564 56616C7565320000

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: 0x00000001 (1)
	    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: Byte String (0x08), Data: BA8D4889753B7414
	    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b4faee10-aa2a-4446-8ad4-0881f3422959
	      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: Byte String (0x08), Data: 88FA2F142C615EDB
	    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b4faee10-aa2a-4446-8ad4-0881f3422959
	      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2

```
42007801000001304200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D02000000040000000200000000042000F01000000704200
5C05000000040000000F00000000420093080000008BA8D4889753B741442007901000000048420094
07000000246234666165653130 2D616132612D343434362D386164342D30383831663334323239353 9
```

```
42007801000001304200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000020000000042000F01000000704200
5C0500000004000000 0F00000000420093080000008BA8D4889753B741442007901000000048420094
0700000024623466616565313 02D616132612D343434362D386164342D303838316633343232393539
0000000042000A070000000C782D617474726962757465310000000042000F010000007042005C0500
0000040000000F00000000420093080000000888FA2F142C615EDB420079010000004842009407 0000
00246234666165653130 2D616132612D343434362D386164342D30383831663334323239353900000 0
0042000A070000000C782D61747472696275746532 00000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E7
(Fri Apr 27 10:12:23 CEST 2012)

    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: Byte String (0x08), Data:
BA8D4889753B7414

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b4faee10-
aa2a-4446-8ad4-0881f3422959

      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: Byte String (0x08), Data: 88FA2F142C615EDB Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b4faee10-aa2a-4446-8ad4-0881f3422959 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 42007B01000001A042007A0100000048420069010000002042006A02000000040000000100000000042 006B02000000040000000100000000420092090000000800000004F9A54E742000D02000000040000 0002000000000042000F01000000A042005C0500000004000000F000000004200930800000008BA8D48 89753B741442007F0500000004000000000000000042007C0100000068420094070000002462346661 656531302D616132612D343434362D386164342D30383831663334323239353900000000420008010 0 00003042000A070000000C782D6174747269627574653100000000042000B070000000E4D6F64696669 656456616C7565310000042000F01000000A042005C0500000004000000F0000000042009308000000 0888FA2F142C615EDB42007F0500000004000000000000000042007C0100000068420094070000002 4 62346661656531302D616132612D343434362D386164342D303838316633343232393539000000004 2 0008010000003042000A070000000C782D6174747269627574653200000000042000B070000000E4D6F 646966696564 56616C7565320000
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: 0x00000001 (1) Tag: 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: b4faee10-
aa2a-4446-8ad4-0881f3422959


42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000001400000000420079010000003042009407000000246234666165653130 2D6161
32612D343434362D386164342D303838316633343232393539000000000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E7
(Fri Apr 27 10:12:23 CEST 2012)
    Tag: 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: b4faee10-
aa2a-4446-8ad4-0881f3422959


42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A54E742000D02000000040000
0001000000042000F01000000584200 5C0500000004000000140000000042007F0500000004000000
00000000042007C010000003042009407000000246234666165653130 2D616132612D343434362D38
6164342D303838316633343232393539000000000
```

9

Client A:

Get (symmetric key)

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: b4faee10-
aa2a-4446-8ad4-0881f3422959
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000484200
5C05000000040000000A000000004200790100000030420094070000002462346661656531302D6161
32612D343434362D386164342D303838316633343232393539000000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 
(Fri Apr 27 10:12:24 CEST 2012)
    Tag: 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: No Cryptographic Object found with given Unique Identifier 42007B01000000D042007A0100000048420069010000002042006A02000000040000000100000000420 06B02000000040000000100000000420092090000000800000004F9A54E842000D02000000040000000 10000000042000F01000000784200 5C05000000040000000A0000000042007F050000000400000001000000 0042007E050000000400000001000000 0042007D070000003A4E6F2043727970746F677261706869632 04F626A65637420666F756E64207769746820676976656E20556E69717565204964656E74696669657 2000000000000
10	Client A: Destroy (template) In: uuidTemplate Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: d83a3a7e-62a3-4f2b-bfe7-11544759000d 42007801000000904200770100000038420069010000002042006A020000000400000001000000004200 6B0200000004000000010000000042000D0200000004000000010000000042000F010000004842005C05 0000000400000014000000004200790100000030420094070000002464383361336137652D363261332D3 46632622D626665372D3131353434373539303030640000000000 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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8
(Fri Apr 27 10:12:24 CEST 2012)

    Tag: 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: d83a3a7e-
62a3-4f2b-bfe7-11544759000d
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A54E842000D020000000400000
00010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000
000000000042007C010000003042009407000000246438336133613765 2D363261332D346632622D62
6665372D3131353434373539303030640000000000
```

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:
```

```
0x00000001 (1)

    Tag: 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: d83a3a7e-
62a3-4f2b-bfe7-11544759000d
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
5C0500000004000000A000000004200790100000030420094070000002464383361336137652D3632
61332D346632622D626665372D31313534343735393030306400000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8
(Fri Apr 27 10:12:24 CEST 2012)

    Tag: 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: No
Cryptographic Object found with given Unique Identifier
```

```
42007B01000000D042007A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A54E842000D020000000400000
000100000000042000F01000000784200050500000004000000A0000000042007F0500000004000000
0100000000042007E05000000040000000100000000042007D070000003A4E6F20437279707746F677261
70686963204F626A65637420666F756E6420776974682067697656E20556E697175652049646 56E74
```

	6966696572000000000000

3.1.5 Test Case: Register / Destroy Secret Data

In this test 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='00000200' }
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
	    Tag: 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 (Password)

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

          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data:
0x00000002 (Opaque)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
536563726574506173737776F7264
```

```
42007801000001004200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000B84200
5C0500000004000000030000000042007901000000A042005705000000040000000700000000420091
0100000038420008010000003042000A070000001843727970746F67726170686963205573616765520
4D61736B42000B02000000040000000200000000420085010000004842008605000000040000000100
0000004200400100000030420042050000000400000002000000004200450100000018420043080000
000E536563726574506173737776F72640000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8
(Fri Apr 27 10:12:24 CEST 2012)

    Tag: 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: 9e9ed79f-
d8f5-4fea-a93d-e02242dfc1d1
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A54E842000D020000000040000
00010000000042000F010000005842005C0500000004000000030000000042007F0500000004000000
000000000042007C010000003042009407000000243965396564373966 2D643866352D346665612D61
```

	3933642D653032323432646663316431000000000

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: 0x00000001 (1)
	    Tag: 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: 9e9ed79f-d8f5-4fea-a93d-e02242dfc1d1
	42007801000000904200770100000038420069010000002042006A02000000040000000100000000420006B0200000004000000010000000042000D0200000004000000010000000042000F010000004842005C050000000400000014000000004200790100000030420094070000002439653965643739662D643866352D346665612D613933642D653032323432646663316431000000000
	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: 0x00000001 (1)
	    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8

	(Fri Apr 27 10:12:24 CEST 2012) Tag: 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: 9e9ed79f-d8f5-4fea-a93d-e02242dfc1d1 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000010000000042009209000000080000000004F9A54E842000D0200000004000000010000000042000F01000000058420005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002439653965643739662D643866352D346665612D613933642D65303232343264666331643100000000

3.2 Test Case: Asynchronous Locate

This test 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 Canceled, before the key is finally destroyed.

This test case shows the use of two clients with the same assumptions as in the test case described in Section . 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 asynchronously to the Locate requests, the client is permitted to skip the requests illustrated at time 7 and 8.

Time	Request/Response messages
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: 
0x00000001 (1)

    Tag: 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
```

```
42007801000001904200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000001484200
5C050000000400000001000000004200790100000130420057050000000400000002000000000420091
0100000118420008010000003042000A070000001743727970746F6772617068696320416C676F7269
74686D0042000B050000000400000003000000004200080100000003042000A0700000014437279707
46F6772617068696320C656E677468000000000042000B020000000400000080000000004200080100000
003842000A07000000044E616D650000000042000B0100000020420055070000000044B657931000000
00420054050000000400000001000000004200080100000003042000A0700000018437279707 46F6772
617068696320557361676520 4D61736B42000B020000000400000004000000004200080100000002842
000A070000000C4F626A6563742047726F75700000000042000B070000000647726F7570310000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8
(Fri Apr 27 10:12:24 CEST 2012)
    Tag: 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: cf22ca7d-
e68c-42d8-bf83-3a98e562f945
```

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A54E842000D0200000004000
00001000000000042000F010000006842005C0500000004000000010000000042007F0500000004000000
0000000000042007C01000000404200570500000004000000020000000042009407000000024636632 32
636137642D653638632D343264382D626638332D336139386535363266393435 00000000
```

1 Client B:

Locate (symmetric key by name)

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

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

```
42007801000000E04200770100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420007060000000800000000000000142000D020000000400000
0001000000000042000F01000000088420005C0500000004000000080000000042007901000000070420008
010000002842000A070000000B4F626A656374205479706500000000042000B050000000400000002
00000000420008010000003842000A07000000044E616D650000000042000B010000002042005507000
0000044B657931000000004200540500000004000000010000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 
(Fri Apr 27 10:12:24 CEST 2012)
    Tag: 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 
(Operation Pending)
    Tag: Asynchronous Correlation Value (0x420006), Type: Byte String (0x08), 
Data: 1C7C3710D40D90B8
```

```
42007B010000008842007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A54E842000D020000000400000
0001000000000042000F010000003042005C0500000004000000080000000042007F050000000400000000
0200000000420006080000000081C7C3710D40D90B8
```

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: 
0x00000001 (1)
```

```
    Tag: 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: Byte String (0x08), 
Data: 1C7C3710D40D90B8
```

```
42007801000000704200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000284200
5C0500000004000000 1A000000004200790100000010420006080000000 81C7C3710D40D90B8
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 
(Fri Apr 27 10:12:24 CEST 2012)

    Tag: 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: cf22ca7d-
e68c-42d8-bf83-3a98e562f945
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A54E842000D020000000040000
00010000000042000F01000000584 2005C0500000004000000080000000042007F0500000004000000
0000000000 42007C010000003042009407000000246366323261 37642D653638632D343264382D62
6638332D336139386535363266393435 00000000
```

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: 
0x00000001 (1)
    Tag: 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: cf22ca7d-
e68c-42d8-bf83-3a98e562f945
```

```
4200780100000090420077010000003842006901000000204200 6A0200000004000000010000000042
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 
(Fri Apr 27 10:12:24 CEST 2012)
    Tag: 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: cf22ca7d-e68c-42d8-bf83-3a98e562f945
      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 (Raw)
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: CC9E3B20F5C4FC4D1298F68D0B7DE65B
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
```

```
42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A54E842000D020000000400000
00010000000042000F01000000C842005C0500000004000000A000000042007F050000000400000000
00000000042007C01000000A042005705000000040000000200000000420094070000002463663232
636137642D653638632D343264382D626638332D3361393865353632663934350000000042008F0100
000058420040010000005042004205000000040000000100000000420045010000001842004308000000
0010CC9E3B20F5C4FC4D1298F68D0B7DE65B42002805000000040000000300000000042002A02000000
040000008000000000
```

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: 
0x00000001 (1)

    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
```

```
42007801000000D04200770100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420007060000000800000000000000014200 0D02000000040000
0001000000000042000F010000007842005C050000000400000008000000004200790100000060420008
010000002842000A070000000B4F626A656374205479706500000000000042000B050000000400000002
00000000420008010000002842000A070000000C4F626A6563742047726F75700000000042000B0700
00000647726F7570310000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 
(Fri Apr 27 10:12:24 CEST 2012)

    Tag: 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 (Operation Pending) Tag: Asynchronous Correlation Value (0x420006), Type: Byte String (0x08), Data: 57BE82A57D3D14E6 42007B010000008842007A0100000048420069010000002042006A0200000004000000010000000042 006B020000000400000001000000004200920900000008000000004F9A54E842000D020000000400000 00010000000042000F010000003042005C050000000400000008000000042007F05000000040000000 020000000042000608000000857BE82A57D3D14E6
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: 0x00000001 (1) Tag: 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: Byte String (0x08), Data: 57BE82A57D3D14E6 420078010000007042007701000000384200690100000020420006A0200000004000000010000000042 006B02000000040000000100000000042000D0200000004000000010000000042000F0100000028420O 5C05000000040000001A0000000042007901000000104200060800000000857BE82A57D3D14E6 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: 0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 (Fri Apr 27 10:12:24 CEST 2012) Tag: 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: cf22ca7d-e68c-42d8-bf83-3a98e562f945 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000001000000004200920900000008000000004F9A54E842000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F0500000004000000000000000042007C010000003042009407000000246366323263613764 2D653638632D343264382D626638332D336139386535363266393435000000000
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: 0x00000001 (1) Tag: 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: cf22ca7d-
e68c-42d8-bf83-3a98e562f945
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000484200
5C0500000004000000A000000004200790100000030420094070000002463663232636137642D6536
38632D343264382D626638332D33613938653536326639343500000000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8
(Fri Apr 27 10:12:24 CEST 2012)
    Tag: 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: cf22ca7d-
e68c-42d8-bf83-3a98e562f945
      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 (Raw)
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
CC9E3B20F5C4FC4D1298F68D0B7DE65B
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data:
0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
```

	0x00000080 (128) 42007B01000001204200 7A0100000048420069010000002042006A02000000040000000100000000042 006B0200000004000000010000000042009209000000080000000004F9A54E842000D020000000040000 000100000000042000F01000000C842005C0500000004000000 0A0000000042007F0500000004000000 000000000042007C01000000A04200570500000004000000020000000042009407000000246366323 2 636137642D653638632D343264382D626638332D3361393865353632663934350000000042008F0100 00005842004001000000504200420500000004000000010000000042004501000000184200430800000 0010CC9E3B20F5C4FC4D1298F68D0B7DE65B4200280500000004000000030000000042002A02000000 040000008000000000

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: 0x00000001 (1)
	    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) 42007801000000E04200770100000048420069010000002042006A0200000004000000010000000042006B020000000400000001000000004200070600000008000000000000000142000D0200000004000000010000000042000F010000008842005C050000000400000008000000004200790100000070420008010000002842000A070000000B4F626A6563742054797065000000000042000B05000000040000000200000000420008010000003842000A07000000044E616D650000000042000B010000002042005507000000044B6579310000000042005405000000040000000100000000 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: 0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 (Fri Apr 27 10:12:24 CEST 2012) Tag: 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 (Operation Pending) Tag: Asynchronous Correlation Value (0x420006), Type: Byte String (0x08), Data: 583B0036C1A2DD01 42007B010000008842007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000001000000004200920900000008000000004F9A54E842000D0200000004000000010000000042000F010000003042005C0500000004000000080000000042007F050000000400000002000000004200060800000008583B0036C1A2DD01
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:
0x00000001 (1)

    Tag: 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: Byte String (0x08),
Data: 583B0036C1A2DD01
```

```
42007801000000704200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F0100000028420
5C050000000400000019000000004200790100000010420006080000000858 3B0036C1A2DD01
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8
(Fri Apr 27 10:12:24 CEST 2012)

    Tag: 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: Byte String (0x08),
```

	Data: 583B0036C1A2DD01 Tag: Cancellation Result (0x420012), Type: Enumeration (0x05), Data: 0x00000001 (Canceled) 42007B01000000A042007A0100000048420069010000002042006A02000000040000000100000000042006B020000000400000001000000004200920900000008000000004F9A54E842000D0200000004000000010000000042000F010000004842005C050000000400000019000000000042007F05000000040000000000000000042007C010000002042000608000000008583B0036C1A2DD0142001205000000040000000100000000
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: 0x00000001 (1) Tag: 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: cf22ca7d-e68c-42d8-bf83-3a98e562f945 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000100000000042000D0200000004000000010000000042000F010000004842005C05000000040000001400000000420079010000003042009407000000246366323263613764 2D6536 38632D343264382D626638332D3361393865353632663934350000000 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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8
(Fri Apr 27 10:12:24 CEST 2012)

    Tag: 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: cf22ca7d-
e68c-42d8-bf83-3a98e562f945



42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042
006B02000000040000000100000000420092090000000800000004F9A54E842000D020000000400000
00010000000042000F01000000058420005C05000000040000001400000000042007F050000000400000000
000000000042007C0100000030420094070000002463663232636137642D653638632D343264382D62
6638332D3361393865353632663934350000000
```

4 Key Life Cycle Support

4.1 Test Case: Revoke Scenario

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

Time	Request/Response messages

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

```
42007801000001604200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420000D0200000004000000010000000042000F01000001184200
5C0500000004000000010000000042007901000001004200570500000004000000020000000420091
01000000E8420008010000003042000A07000000174372797074 6F6772617068696320416C676F7269
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8
(Fri Apr 27 10:12:24 CEST 2012)

    Tag: 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: 668eff89-3010-4258-bc0e-8c402309c746 42007B01000000C042007A0100000048420069010000002042006A02000000040000000100000000042 006B02000000040000000100000000420092090000000800000004F9A54E842000D0200000004000000 0010000000042000F010000006842005C0500000004000000010000000042007F050000000400000000 00000000042007C010000004042005705000000040000000200000000420094070000002436363865 666638392D333031302D343235382D626330652D38633430323330396337343600000000
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: 0x00000001 (1) Tag: 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: 668eff89-3010-4258-bc0e-8c402309c746 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042 006B0200000004000000010000000042000D0200000004000000010000000042000F01000000584200 5C05000000040000000B000000004200790100000040420094070000002436363865666638392D3330 31302D343235382D626330652D38633430323330396337343600000000042000A070000000553746174

```
65000000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8
(Fri Apr 27 10:12:24 CEST 2012)
    Tag: 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: 668eff89-
3010-4258-bc0e-8c402309c746
      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)
```

```
42007B01000000D842007A0100000048420069010000002042006A02000000040000000100000000042
006B020000000400000001000000004200920900000008000000004F9A54E842000D02000000040000
0001000000000042000F010000008042005C0500000004000000B000000000042007F0500000004000000
000000000042007C010000005842009407000000243636386566638392D333031302D343235382D62
6330652D38633430323330396337343600000000420008010000002042000A070000000553746174 65
00000042000B050000000400000001000000000
```

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: 
0x00000001 (1)

    Tag: 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: 668eff89-
3010-4258-bc0e-8c402309c746
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000001200000000420079010000003042009407000000243636386566663839 2D3330
31302D343235382D626330652D3863343032333039633734360000000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 
(Fri Apr 27 10:12:24 CEST 2012)

    Tag: 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: 668eff89-3010-4258-bc0e-8c402309c746 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042 006B020000000400000001000000004200920900000008000000004F9A54E842000D0200000004000000 0001000000000042000F010000005842005C0500000004000000120000000042007F05000000040000000 0000000000042007C0100000030420094070000002436363865666638392D333031302D343235382D62 6330652D3863343032333039633734360000000
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: 0x00000001 (1) Tag: 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: 668eff89-3010-4258-bc0e-8c402309c746 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State 42007801000000A042007701000000384200690100000020420006A0200000004000000010000000042 006B020000000400000001000000000042000D0200000004000000010000000042000F01000000584200 5C05000000040000000B000000004200790100000040420094070000002436363865666638392D3330 31302D343235382D626330652D38633430323330396337343600000000042000A070000000553746174 65000000

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 
(Fri Apr 27 10:12:24 CEST 2012)
    Tag: 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: 668eff89-
3010-4258-bc0e-8c402309c746
      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)
```

```
42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042009209000000080000000004F9A54E842000D0200000004000000
0001000000042000F01000000080042005C0500000004000000000B000000042007F0500000004000000
00000000000042007C010000005842009407000000243636386566663839 2D333031302D343235382D62
6330652D3863343032333039633734360000000004200080100000002042000A07000000055374617465
00000042000B05000000040000000200000000
```

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: 
0x00000001 (1)
    Tag: 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)
```

```
42007801000000D04200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000884200
5C050000000400000008000000004200790100000070420008010000002842000A070000000B4F626A
6563742054797065000000000042000B0500000004000000020000000042000801000000384200 0A07
000000044E616D650000000042000B01000000204200550700000004 4B65793100000000420054 0500
0000040000000100000000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 
(Fri Apr 27 10:12:24 CEST 2012)

    Tag: 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: 668eff89-
3010-4258-bc0e-8c402309c746
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A54E842000D020000000400000
0001000000000042000F010000005842005C05000000040000000800000000042007F0500000004000000
000000000042007C0100000030420094070000002436363865666638392D333031302D343235382D62
6330652D386334303233303963373436000000000
```

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: 
0x00000001 (1)

    Tag: 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: 668eff89-
3010-4258-bc0e-8c402309c746
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F010000004842000
5C05000000040000000A000000004200790100000030420094070000002436363865666638392D3330
31302D343235382D626330652D3863343032333039633734360000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 
(Fri Apr 27 10:12:24 CEST 2012)
    Tag: 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: 668eff89-
3010-4258-bc0e-8c402309c746
      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 (Raw)
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 
9C7D7C4FD2076F1909A6BA4342CAB1DE
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 
0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 
0x00000080 (128)
```

```
42007B010000012042007A0100000048420069010000002042006A02000000040000000100000000042
```

	006B020000000040000000010000000042009209000000008000000004F9A54E842000D02000000040000 0001000000000042000F01000000C842005C0500000000400000000A0000000042007F0500000000400000 000000000042007C01000000A04200570500000000400000000200000000420094070000002436363865 666638392D333031302D343235382D626330652D38633430323330396337343600000000042008F0100 0000584200400100000050420042050000000040000000100000000420045010000001842004308000000 00109C7D7C4FD2076F1909A6BA4342CAB1DE42002805000000004000000030000000042002A02000000 040000008000000000
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: 0x00000001 (1) Tag: 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: 668eff89-3010-4258-bc0e-8c402309c746 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) 42007801000000B84200770100000038420069010000002042006A0200000000400000000100000000042 006B02000000004000000010000000042000D02000000004000000010000000042000F01000000704200 5C05000000004000000130000000042007901000000584200940700000024363638656666383392D3330 31302D343235382D626330652D38633430323330396337343600000000042008101000000104200820 5 00000004000000020000000042002109000000008000000000000006 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: 0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 (Fri Apr 27 10:12:24 CEST 2012) Tag: 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: 668eff89-3010-4258-bc0e-8c402309c746 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000010000000042009209000000080000000004F9A54E842000D0200000004000000010000000042000F010000005842005C0500000004000000130000000042007F0500000004000000000000000042007C010000003042009407000000243636386566663839 2D333031302D343235382D626330652D386334303233303963373436 00000000
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: 0x00000001 (1) Tag: 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: 668eff89-3010-4258-bc0e-8c402309c746
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
```

```
42007801000000A042007701000000384200690100000020042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000584200
5C0500000004000000B000000004200790100000040420094070000002436363865666638392D3330
31302D343235382D626330652D3863343032333039633734360000000042000A070000000553746174
65000000
```

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: 0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 (Fri Apr 27 10:12:24 CEST 2012)
    Tag: 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: 668eff89-3010-4258-bc0e-8c402309c746
      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)
```

<table>
<tr>
<td></td>
<td><pre>
42007B01000000D842007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A54E842000D0200000004000
00001000000042000F01000000804 2005C050000000400000000B000000000042007F0500000004000000
000000000042007C010000005842009407000000243636386566663839 2D333031302D343235382D62
6330652D38633430323330396337343600000000420008010000002042000A07000000055374617465
00000042000B05000000040000000400000000
</pre></td>
</tr>
<tr>
<td>8</td>
<td>
Client A:

Get attribute list

In: uuidKey

<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:
0x00000001 (1)

    Tag: 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: 668eff89-
3010-4258-bc0e-8c402309c746
</pre>

<pre>
420078010000009042007701000000384200690100000020 42006A02000000040000000100000000042
006B020000000400000001000000042000D020000000400000001000000042000F01000000484200
5C050000000400000000C00000000420079010000003042009407000000243636386566663839 2D3330
31302D343235382D626330652D3863343032333039633734360000000
</pre>

Out: uuidKey, attributes = { * }
</td>
</tr>
</table>

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8
(Fri Apr 27 10:12:24 CEST 2012)

    Tag: 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: 668eff89-
3010-4258-bc0e-8c402309c746

      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: Lease Time

      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
```

	42007B010000023842007A0100000048420069010000002042006A0200000004000000010000000042 006B02000000040000000100000000420092090000000800000004F9A54E842000D020000000400000 00010000000042000F01000001E042005C0500000004000000C000000042007F0500000004000000 00000000042007C01000001B842009407000000243636386566638392D333031302D343235382D62 6330652D38633430323330396337343600000000042000A070000001443727970746F677261706869 63 204C656E677468000000042000A07000000174372797074 6F6772617068696320416C676F72697468 6D0042000A070000000553746174650000042000A070000001A436F6D70726F6D697365204F636375 7272656E636520446174650000000000042000A070000000F436F6D70726F6D697365204461746500 42000A070000000644696765737400042000A070000000A4C656173652054696D65000000000000042 000A070000000C496E697469616C204461746500000000042000A070000000F41637469766174696F6E 204461746500042000A07000000115265766F636174696F6E20526561736F6E000000000000042000A 070000001155 6E697175652049646 56E74696669657200000000000000042000A07000000044E616D65 00000000042000A0700000018437279707 46F677261706869632055736167 65204D61736B42000A0700 00000B4F626A65637420547970650000000000042000A07000000104C617374204368616E6765204461 7465

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: 0x00000001 (1)
	    Tag: 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: 668eff89-3010-4258-bc0e-8c402309c746
	      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
	
	42007801000000A042007701000000384200690100000020 42006A0200000004000000010000000042
	006B02000000040000000100000000 42000D0200000004000000010000000042000F01000000584200
	5C05000000040000000B00000000420079010000004042009407000000243636386566638392D3330
	31302D343235382D626330652D38633430323330396337343600000000042000A070000000553746174
	65000000

	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: 0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 (Fri Apr 27 10:12:24 CEST 2012) Tag: 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: 668eff89-3010-4258-bc0e-8c402309c746 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) 42007B01000000D842007A0100000048420069010000002042006A02000000040000000100000000042006B02000000040000000100000000420092090000000800000004F9A54E842000D0200000004000000010000000042000F01000000804200 5C05000000040000000B000000042007F05000000040000000000000000042007C0100000058420094070000002436363865666638392D333031302D343235382D626330652D386334303233303963373436000000004200080100000020 42000A07000000055374617465000000042000B05000000040000000400000000

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:
0x00000001 (1)

    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: Byte String (0x08), Data:
23A177FAA569463C

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 668eff89-
3010-4258-bc0e-8c402309c746

      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: Byte String (0x08), Data:
9B898DC0577F8080

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 668eff89-
3010-4258-bc0e-8c402309c746

      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
```

```
42007801000001604200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000020000000042000F01000000884200
5C05000000040000000D000000004200930800000000823A177FAA569463C420079010000006042009
4
```

3235382D626330652D38633430323330396337343600000000420008010000002842000A070000000C
782D6174747269627574653200000000042000B07000000006566 16C7565320000

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: 0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E8 (Fri Apr 27 10:12:24 CEST 2012)
    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: Byte String (0x08), Data: 23A177FAA569463C
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 668eff89-3010-4258-bc0e-8c402309c746
      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: Byte String (0x08), Data: 9B898DC0577F8080
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
```

	Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 668eff89-3010-4258-bc0e-8c402309c746 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 42007B010000019042007A0100000048420069010000002042006A02000000040000000100000000042 006B0200000004000000010000000042009209000000080000000004F9A54E842000D020000000400000 00020000000042000F01000000984200 5C05000000040000000D00000000420093080000000823A177 FAA569463C42007F0500000004000000000000000042007C010000006042009407000000243636386 5 666638392D333031302D343235382D626330652D38633430323330396337343600000000420008010 0 00002842000A070000000C782D6174747269627574653100000000042000B070000000656616C756531 000042000F010000009842005C050000000400000000D000000004200930800000000 89B898DC0577F80 8042007F0500000004000000000000000042007C010000006042009407000000243636386566663839 2D333031302D343235382D626330652D38633430323330396337343600000000420008010000002842 000A070000000C782D6174747269627574653200000000042000B070000000656616C7565320000
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: 0x00000001 (1) 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: Byte String (0x08), Data: 0752C951BB9926CC Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 668eff89-3010-4258-bc0e-8c402309c746 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: Byte String (0x08), Data:
33F55C8D7E6CAFBF

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 668eff89-
3010-4258-bc0e-8c402309c746

      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
```

```
42007801000001704200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000020000000042000F01000000904200
5C0500000004000000E000000004200930800000008 0752C951BB9926CC42007901000000684200094
07000000243636386566663839 2D333031302D343235382D626330652D38633430323330396337343 6
0000000042000801000000030 42000A070000000C782D617474726962757465310000000042000B0700
00000E4D6F646966696564 56616C75653100004 2000F010000009042005C050000000 4000000 0E0000
00004200930800000008 33F55C8D7E6CAFBF42007901000000684200940700000024363638656666 38
392D333031302D343235382D626330652D3863343032333039633734360000000042000801000000 30
42000A070000000C782D6174747269627574653200000000042000B070000000E4D6F64696669656456
616C7565320000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9
(Fri Apr 27 10:12:25 CEST 2012)
```

	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: Byte String (0x08), Data: 0752C951BB9926CC Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 668eff89-3010-4258-bc0e-8c402309c746 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: Byte String (0x08), Data: 33F55C8D7E6CAFBF Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 668eff89-3010-4258-bc0e-8c402309c746 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 42007B01000001A042007A0100000048420069010000002042006A0200000004000000010000000042 006B02000000040000000100000000420092090000000800000004F9A54E942000D0200000004000 0002000000000042000F01000000A042005C0500000004000000E00000000420093080000000080752C9 51BB9926CC42007F050000000400000000000000042007C0100000068420094070000002436363865 666638392D333031302D343235382D626330652D38633430323330396337343600000000420008010 0 00003042000A070000000C782D61747472696275746531000000000042000B070000000E4D6F64696669 656456616C75653100000042000F01000000A042005C0500000004000000E000000004200930800000 0 0833F55C8D7E6CAFBF42007F050000000400000000000000042007C0100000068420094070000024 3636386566638392D333031302D343235382D626330652D38633430323330396337343600000000042 000801000000003042000A070000000C782D61747472696275746532000000000042000B070000000E4D6F 646966696564566 16C7565320000
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: 0x00000001 (1)
    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: Byte String (0x08), Data: A3EB249B495E8AD2
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 668eff89-3010-4258-bc0e-8c402309c746
      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: Byte String (0x08), Data: C1FE7B3B4C977730
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 668eff89-3010-4258-bc0e-8c402309c746
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: x-attribute2
```

```
42007801000001304200770100000038420069010000002042006A020000000400000001000000042
006B02000000040000000100000000042000D0200000004000000020000000042000F01000000704200
5C0500000004000000F000000004200930800000008A3EB249B495E8AD242007901000000048420094
07000000243636386566638392D333031302D343235382D626330652D3863343032333039633734366
000000042000A070000000C782D61747472696275746531000000042000F01000000704200 5C0500
000004000000F000000004200930800000008C1FE7B3B4C97773042007901000000048420094070000
00243636386566638392D333031302D343235382D626330652D386334303233303963373436000000
0042000A070000000C782D617474726962757465320000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9
(Fri Apr 27 10:12:25 CEST 2012)

    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: Byte String (0x08), Data:
A3EB249B495E8AD2

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 668eff89-
3010-4258-bc0e-8c402309c746

      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: Byte String (0x08), Data:
C1FE7B3B4C977730

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 668eff89-
```

```
3010-4258-bc0e-8c402309c746

      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
```

```
42007B01000001A042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A54E942000D02000000040000
0002000000000042000F01000000A042005C05000000004000000000F00000000420093080000008A3EB24
9B495E8AD242007F050000000400000000000000000042007C0100000068420094070000002436363865
666638392D333031302D343235382D626330652D38633430323330396337343600000000004200080100
00003042000A070000000C782D617474726962757465310000000042000B070000000E4D6F64696669
656456616C7565310000042000F01000000A042005C0500000000400000000F000000004200930800000
08C1FE7B3B4C97773042007F050000000400000000000000000042007C01000000684200940700000024
36363865666638392D333031302D343235382D626330652D38633430323330396337343600000000042
00080100000003042000A070000000C782D617474726962757465320000000042000B070000000E4D6F
64696669656456616C7565320000
```

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:
0x00000001 (1)

    Tag: 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: 668eff89-
3010-4258-bc0e-8c402309c746
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
5C0500000004000000000A000000004200790100000030420094070000002436363865666638392D3330
31302D343235382D626330652D38633430323330396337343600000000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9
(Fri Apr 27 10:12:25 CEST 2012)
    Tag: 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: 668eff89-
3010-4258-bc0e-8c402309c746
      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 (Raw)
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
9C7D7C4FD2076F1909A6BA4342CAB1DE
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data:
0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000080 (128)
```

```
42007B01000001204200 7A0100000048420069010000002042006A020000000400000001000000000042
```

	00109C7D7C4FD2076F1909A6BA4342CAB1DE42002805000000040000000300000000420002A02000000 04000000800000000
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: 0x00000001 (1) Tag: 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: 668eff89-3010-4258-bc0e-8c402309c746 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042 006B0200000004000000010000000042000D0200000004000000010000000042000F010000004842005C05000000040000001400000000420079010000003042009407000000243636386566638392D3330 31302D343235382D626330652D386334303233303963373436000000000 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:

```
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9
(Fri Apr 27 10:12:25 CEST 2012)

    Tag: 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: 668eff89-
3010-4258-bc0e-8c402309c746



42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A54E942000D020000000040000
0001000000000042000F010000005842005C050000000400000014000000000042007F0500000004000000
00000000000042007C010000003042009407000000243636386566663839 2D333031302D343235382D62
6330652D38633430323330396337343600000000
```

5 Auditing and Reporting

5.1 Test Case: Get Usage Allocation Scenario

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

Time	Request/Response messages

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: 0x00000001 (1)`
	`    Tag: 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)
```

```
42007801000001604200770100000038420069010000002042006A02000000040000000100000000042
006B02000000004000000010000000042000D02000000004000000010000000042000F01000001184200
5C05000000004000000010000000042007901000001004200570500000000400000002000000000420091
01000000E84200080100000030420000A070000000174372797074 6F6772617068696320416C676F7269
```

```
420078010000016042007701000000384200690100000020420006A0200000000400000001000000000042
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9
```

	(Fri Apr 27 10:12:25 CEST 2012) Tag: 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: 2c23217e-f53c-4bdf-ad0a-58a31fd3d4b6 42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000001000000004200920900000008000000004F9A54E942000D0200000004000000010000000042000F010000006842005C0500000004000000010000000042007F0500000004000000000000000042007C010000004042005705000000040000000200000000420094070000002432633233323137652D663533632D346264662D616430612D3538613331666433643462360000000
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: 0x00000001 (1) 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: Byte String (0x08), Data: 369F6802EE57532B Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 2c23217e-

```
f53c-4bdf-ad0a-58a31fd3d4b6

      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: Byte String (0x08), Data:
B7CA806E52825BF4

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 2c23217e-
f53c-4bdf-ad0a-58a31fd3d4b6

      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:
0x000000004F9A5741 (Fri Apr 27 10:22:25 CEST 2012)
```

```
42007801000001684200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000020000000042000F01000000884200
5C0500000004000000D0000000042009308000000008369F6802EE57532B4200790100000060420094
070000002432633233323137652D663533632D346264662D616430612D353861333166643364346236
00000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B0900
000008000000000000000242000F010000009042005C05000000040000000D00000000420093080000
0008B7CA806E52825BF44200790100000068420094070000002432633233323137652D663533632D34
6264662D616430612D35386133316664336434623600000000420008010000003042000A0700000011
50726F746563742053746F70204461746500000000000000042000B0900000008000000004F9A5741
```

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:
0x00000001 (1)
```

```
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9
(Fri Apr 27 10:12:25 CEST 2012)

    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: Byte String (0x08), Data:
369F6802EE57532B

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 2c23217e-
f53c-4bdf-ad0a-58a31fd3d4b6

      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: Byte String (0x08), Data:
B7CA806E52825BF4

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 2c23217e-
f53c-4bdf-ad0a-58a31fd3d4b6

      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:
0x000000004F9A5741 (Fri Apr 27 10:22:25 CEST 2012)
```

```
42007B01000001984200７A0100000048420069010000002042006A0200000004000000010000000042
```

2

Client A:

Add Attribute

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

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
    Tag: 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: 2c23217e-f53c-4bdf-ad0a-58a31fd3d4b6
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Usage Limits
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Usage Limits Total (0x420097), Type: Long Integer (0x03), Data: 0x00000000000003E8 (1000)
          Tag: Usage Limits Unit (0x420098), Type: Enumeration (0x05), Data: 0x00000001 (Byte)
```

```
42007801000000D84200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000904200
5C05000000040000000D000000004200790100000078420094070000002432633233323137652D6635
33632D346264662D616430612D35386133316664336434623600000000420008010000004042000A07
0000000C5573616765204C696D6974730000000042000B010000002042009703000000080000000000
0003E842009805000000040000000100000000
```

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

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9 
(Fri Apr 27 10:12:25 CEST 2012)

    Tag: 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: 2c23217e-
f53c-4bdf-ad0a-58a31fd3d4b6

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

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

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

          Tag: Usage Limits Total (0x420097), Type: Long Integer (0x03), Data: 
0x00000000000003E8 (1000)

          Tag: Usage Limits Count (0x420096), Type: Long Integer (0x03), Data: 
0x00000000000003E8 (1000)

          Tag: Usage Limits Unit (0x420098), Type: Enumeration (0x05), Data: 
0x00000001 (Byte)
```

```
42007B010000010842007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A54E942000D02000000040000
00010000000042000F01000000B042005C050000000400000000D0000000042007F05000000004000000
00000000042007C01000000884200940700000024326332333231376520663533632D346264662D61
6430612D353861333166643364346236000000004200080100000050042000A070000000C5573616765
204C696D6974730000000042000B0100000030420097030000000800000000000003E8420096030000
000800000000000003E84200980500000004000000100000000
```

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:
0x00000001 (1)
    Tag: 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 2042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000884200
5C0500000004000000080000000042007901000000704200080100000028 42000A070000000B4F626A
656374205479706500000000 42000B050000000400000002000000004200080100000038 42000A07
000000044E616D650000000042000B01000000204200550700000004 4B6579310000000042005405 00
00000400000001 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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9
(Fri Apr 27 10:12:25 CEST 2012)

    Tag: 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: 2c23217e-
f53c-4bdf-ad0a-58a31fd3d4b6



42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A54E942000D0200000004000
0000100000000042000F010000005842005C0500000004000000080000000042007F0500000004000000
00000000042007C0100000030420094070000002432633233323137652D663533632D346264662D61
6430612D35386133316664336434623600000000
```

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:
0x00000001 (1)

    Tag: 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: 2c23217e-
f53c-4bdf-ad0a-58a31fd3d4b6
```

```
42007801000000904200770100000038420069010000002042006A020000000400000001000000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000000A000000004200790100000030420094070000002432633233323137652D6635
33632D346264662D616430612D3538613331666433643462360000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9
(Fri Apr 27 10:12:25 CEST 2012)

    Tag: 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: 2c23217e-
f53c-4bdf-ad0a-58a31fd3d4b6

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
50F31013C771AF4448110F695EFA9EC7

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

	0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128) 42007B010000012042007A0100000048420069010000002042006A02000000040000000100000000420 06B0200000004000000010000000042009209000000080000000004F9A54E942000D020000000400000 0010000000042000F01000000C842005C0500000004000000000A0000000042007F050000000400000000 00000000042007C01000000A04200570500000004000000002000000004200940700000024326332333 23137652D663533632D346264662D616430612D35386133316664336434623600000000042008F0100 0000584200400100000050420042050000000400000001000000004200450100000018420043080000 001050F31013C771AF4448110F695EFA9EC7420028050000000400000003000000042002A02000000 04000000800000000
5	Client B: Check Get usage allocation In (header): BatchOrderOption='true' In: uuidKey, UsageLimitsCount='500' In: uuidKey, UsageLimitsCount='500' Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) 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: Byte String (0x08), Data: D35A294F9425F06E Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 2c23217e-f53c-4bdf-ad0a-58a31fd3d4b6 Tag: Usage Limits Count (0x420096), Type: Long Integer (0x03), Data: 0x00000000000001F4 (500) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
80454D8CE4F738FE

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 2c23217e-
f53c-4bdf-ad0a-58a31fd3d4b6

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

```
42007801000001204200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000020000000042000F01000000684200
5C0500000004000000090000000042009308000000008D35A294F9425F06E4200790100000040420094
0700000024326332333231376520D663533632D346264662D616430612D3538613331666433643462336
0000000042009603000000080000000000001F442000F01000000684200 5C050000000400000011000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9
(Fri Apr 27 10:12:25 CEST 2012)

    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: Byte String (0x08), Data:
D35A294F9425F06E

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 2c23217e-
```

	f53c-4bdf-ad0a-58a31fd3d4b6
	  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: Byte String (0x08), Data: 80454D8CE4F738FE
	    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 2c23217e-f53c-4bdf-ad0a-58a31fd3d4b6
	
	42007B01000001304200 7A0100000048420069010000002042006A02000000040000000100000000420 06B02000000040000000100000000420092090000000800000000 4F9A54E942000D0200000004000000020000000042000F01000000684200 5C0500000004000000090000000042009308000000008D35A294F9425F06E42007F050000000400000000000000 0042007C0100000030420094070000002432633233323137652D663533632D346264662D616430612D35386133316664336434623600000000 42000F01000000684200 5C050000000400000011000000004200930800000000880454D8CE4F738FE42007F0500000004000000000000000042007C0100000030420094070000002432633233323137652D663533632D346264662D616430612D3538613331666433643462360000000 0

6	Client A:
	Get usage allocation
	In: uuidKey, UsageLimitsCount='500'
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
	    Tag: 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: 2c23217e-f53c-4bdf-ad0a-58a31fd3d4b6
	      Tag: Usage Limits Count (0x420096), Type: Long Integer (0x03), Data:

```
0x00000000000001F4 (500)
```

```
42007801000000A04200770100000038420069010000002042006A02000000040000000100000000420
06B02000000040000000100000000042000D02000000040000000100000000042000F0100000058420
05C05000000040000001100000000420079010000004042009407000000243263323332313765 2D6635
33632D346264662D616430612D3538613331666433643462360000000042009603000000080000000
000001F4
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9
(Fri Apr 27 10:12:25 CEST 2012)

    Tag: 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: 2c23217e-
f53c-4bdf-ad0a-58a31fd3d4b6
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420
06B02000000040000000100000000420092090000000800000004F9A54E942000D0200000004000
00001000000000042000F010000005842005C050000000400000011000000000042007F050000000400000
0000000000042007C010000003042009407000000243263323332313765 2D663533632D346264662D61
6430612D35386133316664336434623600000000
```

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:
0x00000001 (1)

    Tag: 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)
```

```
42007801000000D04200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000884200
5C05000000040000000800000000420079010000007042000801000000284200 0A070000000B4F626A
6563742054797065000000000042000B05000000040000000200000000420008010000003842000A07
000000044E616D650000000042000B010000002042005507000000044B6579310000000004200540500
0000040000000100000000
```

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: 0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9 (Fri Apr 27 10:12:25 CEST 2012) Tag: 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: 2c23217e-f53c-4bdf-ad0a-58a31fd3d4b6 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000100000000420092090000000800000004F9A54E942000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F0500000004000000000000000042007C0100000030420094070000002432633233323137652D663533632D346264662D616430612D35386133316664336434623600000000
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: 0x00000001 (1) Tag: 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: 2c23217e-

```
f53c-4bdf-ad0a-58a31fd3d4b6
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000484200
5C05000000040000000A0000000042007901000000304200940700000024326332333231 37652D6635
33632D346264662D616430612D35386133316664336434623600000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9
(Fri Apr 27 10:12:25 CEST 2012)

    Tag: 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: 2c23217e-
f53c-4bdf-ad0a-58a31fd3d4b6

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
50F31013C771AF4448110F695EFA9EC7

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

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

	0x00000080 (128) 42007B010000012042007A0100000048420069010000002042006A02000000040000000100000000042 006B02000000040000000100000000420092090000000800000004F9A54E942000D0200000004000000 0010000000042000F01000000C842005C0500000004000000A0000000042007F0500000004000000 0000000000042007C01000000A0420057050000000400000002000000004200940700000024326332333 23137652D663533632D346264662D616430612D35386133316664336434623600000000042008F0100 0000584200400100000050420042050000000400000001000000004200450100000018420043080000 001050F31013C771AF4448110F695EFA9EC7420028050000000400000003000000042002A02000000 040000008000000000

9	Client C:
	Get usage allocation
	In: uuidKey, UsageLimitsCount='500'
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
	    Tag: 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: 2c23217e-f53c-4bdf-ad0a-58a31fd3d4b6
	      Tag: Usage Limits Count (0x420096), Type: Long Integer (0x03), Data: 0x00000000000001F4 (500)
	42007801000000A0420077010000003842006901000000 2042006A02000000040000000100000000042
	006B02000000040000000100000000042000D02000000040000000100000000042000F010000005842 00
	5C050000000400000011000000004200790100000004042009407000000243263323332313765 2D6635
	33632D346264662D616430612D35386133316664336434623600000000042009603000000008000000 00
	000001F4
	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: 0x00000001 (1)
	    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9 (Fri Apr 27 10:12:25 CEST 2012)
	    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000011 (Get Usage Allocation)
	    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed)
	    Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x0000000C (Permission Denied)
	    Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Unable to allocate requested amount
	
	42007B01000000B842007A0100000048420069010000002042006A02000000040000000100000000042
	006B02000000040000000100000000420092090000000800000004F9A54E942000D020000000400000
	00010000000042000F010000006042005C05000000040000001100000000042007F0500000004000000
	010000000042007E050000000400000000C0000000042007D0700000023556E61626C6520746F20616C
	6C6F6361746520726571756573746564420616D6F756E740000000000

10	Client A: Revoke (symmetric key as cessation of operation) and Destroy (symmetric key) In (header): batchOrderOption='TRUE' In: uuidKey, revocationReasonCode='6' In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data:

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

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

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
79B998C5F29465F4

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 2c23217e-
f53c-4bdf-ad0a-58a31fd3d4b6

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

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
B0633F0E41187345

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 2c23217e-
f53c-4bdf-ad0a-58a31fd3d4b6
```

```
42007801000001284200770100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420010060000000800000000000000142000D0200000004000
00020000000042000F010000007042005C0500000004000000130000000042009308000000879B998
C5F29465F44200790100000048420094070000002432633233323137652D663533632D346264662D61
6430612D35386133316664336434623600000000420081010000001042008205000000040000000600
00000042000F01000000584200 5C050000000400000014000000004200930800000008B0633F0E4118
73454200790100000030420094070000002432633233323137652D663533632D346264662D61643061
2D353861333166643364346236000000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9
(Fri Apr 27 10:12:25 CEST 2012)

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
79B998C5F29465F4

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 2c23217e-
f53c-4bdf-ad0a-58a31fd3d4b6

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
B0633F0E41187345

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 2c23217e-
f53c-4bdf-ad0a-58a31fd3d4b6



42007B010000013042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A54E942000D02000000040000
00020000000042000F010000006842005C0500000004000000130000000042009308000000879B998
C5F29465F442007F0500000004000000000000000042007C0100000030420094070000002432633233
323137652D663533632D346264662D616430612D35386133316664336434623600000000042000F0100
00006842005C050000000400000014000000004200930800000008B0633F0E4118734542007F050000
0004000000000000000042007C0100000030420094070000002432633233323137652D663533632D34
6264662D616430612D353861333166643364346236000000000
```

138

139

6 Key Interchange, Key Exchange

6.1 Test Case: Import of a Third-party Key

This test 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: 0x00000001 (1) Tag: 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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
0123456789ABCDEF0123456789ABCDEF

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

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

```
42007801000001104200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000C84200
5C0500000004000000030000000042007901000000B0420057050000000400000002000000000420091
0100000038420008010000003042000A070000001843727970746F6772617068696320557361676520
4D61736B42000B020000000400000004000000000042008F0100000058420040010000005042004205000
000040000000100000000420045010000001842004308000000100123456789ABCDEF0123456789AB
CDEF42002805000000040000000300000000042002A02000000040000008000000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9
(Fri Apr 27 10:12:25 CEST 2012)

    Tag: 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: 3e2629a7-
8b82-4c95-9258-4fd6e6ba96c4
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B020000000400000001000000004200920900000008000000004F9A54E942000D02000000040000
```

```
00010000000042000F01000000058420005C0500000000400000000300000000042007F0500000000400000
00000000042007C01000000304200940700000024336532363239613 72D386238322D346339352D39
3235382D34666436653666261393663340000000
```

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: 
0x00000001 (1)
    Tag: 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: 3e2629a7-
8b82-4c95-9258-4fd6e6ba96c4
      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
```

```
42007801000000C042007701000000384200690100000020420006A020000000040000000100000000042
006B0200000000400000001000000000042000D0200000000400000001000000000042000F01000000784200
5C05000000040000000D000000004200790100000060420094070000002433653236323961372D3862
38322D346339352D393235382D346664366536626139366334000000004200080100000002842000A07
0000000A782D70726F7669646572000000000000042000B0700000007756E6B6E6F776E00
```

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: 0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9 (Fri Apr 27 10:12:25 CEST 2012)
    Tag: 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: 3e2629a7-8b82-4c95-9258-4fd6e6ba96c4
      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
```

```
42007B01000000E042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A54E942000D02000000040000
0001000000000042000F01000000884200 5C0500000004000000 0D0000000042007F0500000004000000
000000000042007C01000000604200940700000024336532363239613 72D386238322D346339352D39
3235382D34666436653662613936633400000000420008010000002842000A070000000A782D70726F
766964657200000000000042000B0700000007756E6B6E6F776E00
```

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: 0x00000001 (1)
    Tag: 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: 3e2629a7-8b82-4c95-9258-4fd6e6ba96c4

      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
```

```
42007801000000C84200770100000038420069010000002042006A020000000400000001000000004200
6B0200000004000000010000000042000D0200000004000000010000000042000F01000000804200
5C0500000004000000E00000000420079010000006842009407000000243365323632396137 2D3862
38322D346339352D393235382D3466643665366261393663340000000042000801000000 3042000A07
0000000A782D70726F766964657200000000000042000B070000000B74686972642070617274790000
000000
```

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: 0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9 (Fri Apr 27 10:12:25 CEST 2012)

    Tag: 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: 3e2629a7-8b82-4c95-9258-4fd6e6ba96c4

      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
```

```
42007B01000000E842007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A54E942000D020000000400000
0001000000000042000F010000009042005C0500000004000000E000000042007F0500000004000000
000000000042007C010000006842009407000000243365323636323961372D386238322D346339352D39
3235382D3466643665366261393663340000000042000801000000030420000A070000000A782D70726F
766964657200000000000042000B070000000B7468697264207061727479000000000
```

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:
0x00000001 (1)

    Tag: 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: 3e2629a7-
8b82-4c95-9258-4fd6e6ba96c4
```

```
420078010000009042007701000000384200690100000020420006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000484200
5C050000000400000014000000004200790100000030420094070000002433653236323961372D3862
38322D346339352D393235382D34666436653662613936633400000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9
(Fri Apr 27 10:12:25 CEST 2012)

    Tag: 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: 3e2629a7-
8b82-4c95-9258-4fd6e6ba96c4



42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A54E942000D02000000040000
000100000000042000F010000005842005C050000000400000014000000000042007F0500000004000000
00000000042007C0100000030420094070000002433653236323961372D386238322D346339352D39
3235382D3466643665366261393663340000000
```

7 Vendor Extensions

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

7.1 Test 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	Request/Response messages

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: 0x00000001 (1)
	    Tag: 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: Vendor Identification (0x42009D), Type: Text String (0x07), Data: Acme

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

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

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



42007801000001604200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000001184200
5C0500000004000000010000000042007901000000C04200570500000004000000020000000042009
101000000A84200080100000030420000A070000001443727970746F67726170686963204C656E677468
0000000042000B020000000400000080000000004200080100000030420000A070000001743727970 74
6F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000801000
0003042000A070000001843727970746F677261706869632055736167652 04D61736B42000B02000000
040000000C000000004200510100000038420 09D070000000441636D650000000042002606000000008
000000000000000042009C010000001001424207000000026E61000000000000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9 
(Fri Apr 27 10:12:25 CEST 2012)

    Tag: 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: bdc90168-5cd3-480c-b900-aa9924861f40 42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042 006B0200000004000000010000000042009209000000080000000004F9A54E942000D020000000400000 0001000000000042000F010000006842005C0500000004000000010000000042007F050000000400000000 000000000042007C010000004042005705000000040000000200000000420094070000002462646339 303136382D356364332D343830632D623930302D6161393932343836316634300000000000
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: 0x00000001 (1) Tag: 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: bdc90168-5cd3-480c-b900-aa9924861f40 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042 006B02000000040000000100000000042000D0200000004000000010000000042000F0100000048420 5C050000000400000014000000004200790100000030420094070000002462646339303136382D3563 64332D343830632D623930302D6161393932343836316634300000000000 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: 0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9 (Fri Apr 27 10:12:25 CEST 2012) Tag: 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: bdc90168-5cd3-480c-b900-aa9924861f40 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000010000000042009209000000080000000004F9A54E942000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002462646339303136382D356364332D343830632D623930302D61613939323438363166343000000000

7.2 Test 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	Request/Response messages
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:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: 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: Vendor Identification (0x42009D), Type: Text String (0x07), Data: Acme
      Tag: Criticality Indicator (0x420026), Type: Boolean (0x06), Data: TRUE
      Tag: Vendor Extension (0x42009C), Type: Structure (0x01), Data:
        Tag: Unknown tag (0x014242), Type: Text String (0x07), Data: na
```

```
42007801000001604200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000001184200
5C05000000040000000100000000420079010000000C0420057050000000400000002000000000420091
01000000A84200080100000030042000A070000001443727970746F6772617068696963204C656E677468
0000000042000B020000000400000008000000000420008010000003042000A07000000174372797074
6F6772617068696320416C676F726974686D0042000B050000000400000003000000000420008010000
003042000A0700000018437279707466F677261706869632055736167652044D61736B42000B02000000
040000000C0000000042005101000000003842009D070000000441636D650000000004200260600000008
00000000000000142009C010000000100142420700000026E61000000000000
```

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: 0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54E9 (Fri Apr 27 10:12:25 CEST 2012)
    Tag: 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
```

```
42007B01000000C042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000080000000004F9A54E942000D020000000040000
00010000000042000F0100000068420005C050000000400000001000000000042007F050000000400000000
0100000000042007E05000000004000000080000000042007D070000002943726974696361616C204D6573
736167652045787465E73696F6E206E6F74207265636F676E697A65640000000000000000
```

8 Asymmetric Keys

Creation of asymmetric keys using the "Create Key Pair" operation and registration of asymmetric keys using the "Register" operation. Relationship management and tracking using the Link attribute.

8.1 Test Case: Create a Key Pair

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

Time	Request/Response messages

0	Create Key Pair
	In: commonAttributes={ CryptographicAlgorithm='RSA', CryptographicLength='1024' }, privateKeyAttributes={ Name={ NameValue='PrivateKey1', NameType='00000001' }, CryptographicUsageMask='00000001' }, publicKeyAttributes={ NameValue='PublicKey1', NameType='00000001' }, 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: 0x00000001 (1)
	    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000002 (Create Key Pair)
	    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	      Tag: Common Template-Attribute (0x42001F), Type: Structure (0x01), Data:
	        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Algorithm
	          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000004 (RSA)
	        Tag: Attribute (0x420008), Type: Structure (0x01), Data:

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

          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000400
(1024)

      Tag: Private Key Template-Attribute (0x420065), Type: Structure (0x01),
Data:

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

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

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

            Tag: Name Value (0x420055), Type: Text String (0x07), Data:
PrivateKey1

            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001
(Uninterpreted Text String)

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

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

          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000001
(Sign)

      Tag: Public Key Template-Attribute (0x42006E), Type: Structure (0x01), Data:

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

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

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

            Tag: Name Value (0x420055), Type: Text String (0x07), Data: PublicKey1

            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001
(Uninterpreted Text String)

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

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

          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000002
(Verify)
```

```
42007801000001E84200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000001A04200
5C0500000004000000020000000042007901000001884200 1F0100000070420008010000003042000A
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA 
(Fri Apr 27 10:12:26 CEST 2012)

    Tag: 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: Private Key Unique Identifier (0x420066), Type: Text String (0x07), 
Data: 7f7ee394-40f9-444c-818c-fb1ae57bdf15

      Tag: Public Key Unique Identifier (0x42006F), Type: Text String (0x07), 
Data: 79c0eb55-d020-43de-b72f-5e18c862647c
```

```
42007B01000000E042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A54EA42000D020000000400000
0001000000042000F010000008842005C0500000004000000020000000042007F050000000400000
0000000000042007C0100000060420066070000002437663765653339342D343066392D343434632D38
3138632D6662316165353762646631350000000042006F0700000024373963306562353352D64303230
2D343364652D623732662D35653138633836323634376300000000
```

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: 
0x00000001 (1)
    Tag: 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: 7f7ee394-40f9-444c-818c-fb1ae57bdf15
```

```
42007801000000F042007701000000384200690100000020420006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000A84200
5C050000000400000008000000004200790100000090420008010000002842000A070000000B4F626A
6563742054797065000000000042000B050000000400000003000000004200080100000058420000A07
000000044C696E6B0000000042000B010000004042004B0500000004000001030000000042004C0700
000024376637656533393422D343066392D343434632D383138632D66623161653537626466313500000
0000
```

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: 
0x00000001 (1)
```

```
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA
(Fri Apr 27 10:12:26 CEST 2012)

    Tag: 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: 79c0eb55-
d020-43de-b72f-5e18c862647c



42007B01000000B042007A01000000484200690100000020420 06A02000000040000000100000000 42
006B0200000004000000010000000042009209000000080000000004F9A54EA42000D0200000004000 0
000100000000042000F010000005842005C05000000040000000800000000042007F0500000004000000
0000000000 42007C0100000030420094070000002437396330656235352D643032302D343364652D62
3732662D35653138633836323634376300000000
```

2

Locate (Private Key)

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

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: 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: 79c0eb55-d020-43de-b72f-5e18c862647c
```

```
42007801000000F04200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000A84200
5C05000000040000000800000000420079010000009042000801000000284200A070000000B4F626A
65637420547970650000000000042000B05000000040000000400000000420008010000005842000A07
000000044C696E6B000000000042000B01000000404200 4B05000000040000010200000000042004C0700
0000243739633065623535 2D643032302D343364652D623732662D356531386338363236343763 0000
0000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA
(Fri Apr 27 10:12:26 CEST 2012)

    Tag: 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: 7f7ee394-
40f9-444c-818c-fb1ae57bdf15
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042009209000000080000000004F9A54EA42000D020000000400000
0001000000000042000F010000005842005C05000000040000000800000000042007F050000000040000000
0000000000042007C010000003042009407000000243766376565333934 2D343066392D343434632D38
3138632D6662316165353762646631350 0000000
```

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: 0x00000001 (1)
    Tag: 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: 7f7ee394-40f9-444c-818c-fb1ae57bdf15
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C0500000004000000140000000042007901000000304200940700000024376637656533393422D3430
66392D343434632D383138632D666231616535376264663135000000000
```

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: 0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA (Fri Apr 27 10:12:26 CEST 2012)
```

	Tag: 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: 7f7ee394-40f9-444c-818c-fb1ae57bdf15 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042 006B02000000040000000100000000420092090000000800000004F9A54EA42000D020000000040000 0001000000000042000F010000005842005C0500000004000000140000000042007F0500000004000000 0000000000042007C010000003042009407000000243766376565333942D343066392D343434632D38 3138632D66623161653537626466313500000000
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: 0x00000001 (1) Tag: 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: 79c0eb55-d020-43de-b72f-5e18c862647c 420078010000009042007701000000384200690100000020420069A0200000004000000010000000042 006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200 5C0500000004000000140000000042007901000000304200940700000024373963306562353352D6430 32302D343364652D623732662D3565313863383632363437630000000

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA
(Fri Apr 27 10:12:26 CEST 2012)
    Tag: 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: 79c0eb55-
d020-43de-b72f-5e18c862647c
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042009209000000080000000004F9A54EA42000D020000000040000
00010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000
00000000000042007C010000003042009407000000243739633065623535352D643032302D343364652D62
3732662D3565313863383632363437630000000000
```

8.2 Test 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	Request/Response messages
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:
0x00000001 (1)

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

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

    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003
(Register)

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

      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000004
(Private Key)

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

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

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

          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000001
(Sign)

      Tag: Private Key (0x420064), Type: Structure (0x01), Data:

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

          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data:
0x00000004 (PKCS#8)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
30820276020100300D06092A864886F70D0101010500048202603082025C02010002818100930451C9
ECD94F5BB9DA17DD09381BD23BE43ECA8C7539F301FC8A8CD5D5274C3E7699DBDC711C97A7AA91E2C5
0A82BD0B1034F0DF493DEC16362427E58ACCE7F6CE0F9BCC617BBD8C90D0094A2703BA0D09EB19D100
5F2FB265526AAC75AF32F8BC782CDED2A57F811E03EAF67A944DE5E78413DCA8F232D074E6DCEA4CEC
9F02030100010281800B6A7D736199EA48A420E4537CA0C7C046784DCBEAA63BAEBC0BC132787449CD
E8D7CAD0C0C863C0FEFB06C3062BEFC50033ECF87B4E33A9BE7BCBC8F1511AE215E80DEB5D8AF2BD31
319D7821196640935A0CD67C94599579F2100D65E038831FDAFB0DBE2BBDAC00A696E67E756350E1C9
9ACE11A36DABAC3ED3E730960059024100DDF672FBCC5BDA3D73AFFC4E791E0C03390224405D69CCAA
BC749FAA0DCD4C2583C71DDE8941A7B9AA030F52EF1451466C074D4D338FE677892ACD9E10FD35BD02
4100A98FBC3ED6B4C6F860F97165AC2F7BB6F2E2CB192A9ABD49795BE5BCF37D8EE69A6E169C24E5C3
2E4E7FA33265461407F952BA49E204818A2F785F113F922B8B0240253F9470390D39049303777DDBC9
750E9D64849CE0903EAE704DC9F589B7680DEB9D609FD5BCD4DECD6F120542E5CFF5D76F2A43C8615F
B5B3A9213463797AA9024100A1DDF023C0CD94C019BB26D09B9E3CA8FA971CB16AA58B9BAF79D6081A
1DBBA452BA53653E2804BA98FF69E8BB1B3A161EA225EA501463216A8DAB9B88A75E5F02406178646E
112CF79D921A8A843F17F6E7FF974F688122365BF6690CDFC996E1890952EB3820DD1890EC1C8619E8
7A2BD38F9D03B37FAC742EFB748C7885942C39

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

```
0x00000004 (RSA)

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

```
420078010000038042007701000000384200690100000020420006A020000000400000001000000042
006B02000000040000000100000000042000D020000000400000001000000042000F01000003384200
5C0500000004000000030000000042007901000003204200570500000004000000040000000420091
010000003842000801000000304200A07000000184372797074F677261706869632055736167652 0
```

```
42007801000003804200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000003384200
5C050000000400000003000000004200790100000320420057050000000400000004000000000420091
010000003842000801000000304200A070000000184372797074F67726170686963205573616765 20
4D61736B42000B020000000400000001000000004200640100002C84200400100002C04200420500
000004000000040000000042004501000002884200430800000027A30820276020100300D06092A8648
86F70D0101010500048202603082025C02010002818100930451C9ECD94F5BB9DA17DD09381BD23BE4
3ECA8C7539F301FC8A8CD5D5274C3E7699DBDC711C97A7AA91E2C50A82BD0B1034F0DF493DEC163624
27E58ACCE7F6CE0F9BCC617BBD8C90D0094A2703BA0D09EB19D1005F2FB265526AAC75AF32F8BC782C
DED2A57F811E03EAF67A944DE5E78413DCA8F232D074E6DCEA4CEC9F0203010001028180 0B6A7D7361
```

	Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 57e3d38c-5532-425a-8bd6-b9bfee93bb0b 42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042006B020000000400000001000000004200920900000008000000004F9A54EA42000D0200000004000000010000000042000F010000005842005C050000000400000003000000000042007F0500000004000000000000000042007C01000000304200940700000024353765336433386632D353533322D343235612D386264362D623962666565393362623062000000000
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: 0x00000001 (1) Tag: 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: 57e3d38c-5532-425a-8bd6-b9bfee93bb0b

      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 (X.509)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 
30819F300D06092A864886F70D010101050003818D0030818902818100930451C9ECD94F5BB9DA17DD
09381BD23BE43ECA8C7539F301FC8A8CD5D5274C3E7699DBDC711C97A7AA91E2C50A82BD0B1034F0DF
493DEC16362427E58ACCE7F6CE0F9BCC617BBD8C90D0094A2703BA0D09EB19D1005F2FB265526AAC75
AF32F8BC782CDED2A57F811E03EAF67A944DE5E78413DCA8F232D074E6DCEA4CEC9F0203010001

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

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

```
420078010000020842007701000000384200690100000020420006A020000000400000001000000000 42
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA 
(Fri Apr 27 10:12:26 CEST 2012)

    Tag: 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: 51b35b14-
8551-4798-a450-4eea4e23e38d
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A54EA42000D020000000400000
0001000000000042000F010000005842005C0500000004000000030000000042007F0500000004000000
0000000000042007C010000003042009407000000243531623335623134 2D383535312D343739382D61
3435302D34656561346532336533386400000000
```

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:
0x00000001 (1)

    Tag: 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: 57e3d38c-
5532-425a-8bd6-b9bfee93bb0b

      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: 51b35b14-8551-4798-a450-4eea4e23e38d
```

```
42007801000000F04200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000A84200
5C0500000004000000D000000004200790100000090420094070000002435376533643338632D3535
33322D343235612D386264362D623962666565393362623062000000004200080100000058420000A07
000000044C696E6B000000042000B01000000404204B050000000400000102000000042004C0700
000024353162333562313342D383535312D343739382D613435302D346565613465323365333864000
0000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA
(Fri Apr 27 10:12:26 CEST 2012)

    Tag: 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: 57e3d38c-
5532-425a-8bd6-b9bfee93bb0b

      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: 51b35b14-8551-4798-a450-4eea4e23e38d
```

	42007B01000001104200 7A01000000484200690100000020420 06A020000000400000001000000 00042 006B020000000400000001000000004200920900000008000000004F9A54EA42000D020000000040000 0001000000000042000F01000000B842005C05000000040000000D000000000042007F0500000000400000 0 00000000042007C010000009042009407000000243537653364333863 2D353533322D343235612D38 6264362D623962666565393362623062000000004200080100000058 42000A07000000044C696E6B00 000000042000B010000004042004B050000000400000102000000000 42004C07000000243531623335 62 31342D383535312D343739382D613435302D34656561346532336533386400000000

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: 0x00000001 (1)
	    Tag: 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: 57e3d38c-5532-425a-8bd6-b9bfee93bb0b
	42007801000000F04200770100000038420069010000002042006A0200000004000000010000000042
	006B02000000040000000100000000042000D0200000004000000010000000042000F01000000A84200
	5C05000000040000000800000000420079010000009042000801000000284 2000A070000000B4F626A
	656374205479706500000000000042000B05000000040000000300000000420008010000005842000A07
	000000044C696E6B0000000042000B010000004042004B05000000040000010300000000 42004C0700

```
00002435376533643338632D353533322D343235612D386264362D623962666565393362623062000000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA 
(Fri Apr 27 10:12:26 CEST 2012)
    Tag: 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: 51b35b14-
8551-4798-a450-4eea4e23e38d
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420
06B02000000040000000100000000420092090000000800000004F9A54EA42000D020000000400000
00010000000042000F010000005842005C0500000004000000080000000042007F0500000004000000
000000000042007C0100000030420094070000002435316233356231342D383535312D343739382D61
3435302D34656561346532336533386400000000
```

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: 
0x00000001 (1)
    Tag: 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: 51b35b14-8551-4798-a450-4eea4e23e38d
```

```
42007801000000F04200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000A84200
5C0500000004000000080000000042007901000000904200080100000028420000A070000000B4F626A
6563742054797065000000000042000B05000000040000000400000000420008010000005842000A07
000000044C696E6B000000000042000B01000000404200004B05000000040000010200000000042004C0700
00002435316233356231342D383535312D343739382D613435302D346565613465323365333864000000
0000
```

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: 
0x00000001 (1)
```

```
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA
(Fri Apr 27 10:12:26 CEST 2012)

    Tag: 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: 57e3d38c-
5532-425a-8bd6-b9bfee93bb0b
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A54EA42000D02000000040000
00010000000042000F01000000584200 5C050000000400000008000000042007F050000000400000000
```

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:
0x00000001 (1)

    Tag: 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: 57e3d38c-
5532-425a-8bd6-b9bfee93bb0b
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000001400000000420079010000003042009407000000243537653364333863 2D3535
33322D343235612D386264362D623962666565393362623062 00000000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA
(Fri Apr 27 10:12:26 CEST 2012)
    Tag: 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: 57e3d38c-
5532-425a-8bd6-b9bfee93bb0b
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000004000000010000000042009209000000080000000004F9A54EA42000D02000000040000
000100000000042000F01000000584200 5C05000000040000001400000000042007F0500000004000000
00000000042007C0100000030420094070000002435376533643338632D353533322D343235612D38
6264362D6239626666565393362623062 00000000
```

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:
0x00000001 (1)

    Tag: 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: 51b35b14-
8551-4798-a450-4eea4e23e38d



42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000484200
5C05000000040000001400000000420079010000003042009407000000243531623335623134 2D3835
35312D343739382D613435302D34656561346532336533386400000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA
(Fri Apr 27 10:12:26 CEST 2012)

    Tag: 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: 51b35b14-
8551-4798-a450-4eea4e23e38d



42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A54EA42000D02000000040000
```

	00010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000 000000000042007C0100000030420094070000002435316233356231342D383535312D343739382D61 3435302D34656561346532336533386400000000

174

175

9 Key Roll-over

These test 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 Test 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	Request/Response messages

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: 0x00000001 (1)`
	`    Tag: 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)
```

```
42007801000001604200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000001184200
5C0500000004000000010000000042007901000001004200570500000004000000020000000420091
01000000E8420008010000003042000A07000000174372797074F6772617068696320416C676F7269
74686D0042000B05000000040000000300000000420008010000003042000A070000001443727970746
6F6772617068696320 4C656E677468000000000042000B02000000040000008000000000420008010000
003042000A07000000184372797074 6F6772617068696320557361676520 4D61736B42000B02000000
040000000C00000000420008010000003842000A07000000044E616D650000000042000B0100000020
42005507000000872656B65794B6579420054050000000400000001000000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA
(Fri Apr 27 10:12:26 CEST 2012)
```

```
    Tag: 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: 964d3dd2-5f06-4529-8bb8-ae630b6ca2e0
```

```
42007B01000000C042007A0100000048420069010000002042006A02000000040000000100000000420
06B0200000004000000010000000042009209000000080000000004F9A54EA42000D02000000040000
0001000000000042000F01000000684200５C0500000004000000010000000042007F050000000400000
00000000000042007C01000000404200570500000004000000020000000042009407000000243936346
4336464322D356630362D343532392D386262382D6165363330623663613265300000000000
```

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: 0x00000001 (1)
    Tag: 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)
```

```
42007801000000A04200770100000038420069010000002042006A020000000400000001000000004200
6B020000000400000001000000042000D020000000400000001000000042000F01000000584200
5C050000000400000008000000004200790100000040420008010000003842000A070000000044E616D
650000000042000B0100000020420055070000000872656B65794B657942005405000000040000000100000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA 
(Fri Apr 27 10:12:26 CEST 2012)
    Tag: 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: 964d3dd2-
5f06-4529-8bb8-ae630b6ca2e0
```

```
42007B01000000B042007A01000000484200690100000020420006A020000000400000001000000042
006B020000000400000001000000004200920900000008000000004F9A54EA42000D0200000004000
000010000000042000F010000005842005C050000000400000008000000042007F0500000004000000
0000000000042007C0100000030420094070000002439363464336464322D356630362D343532392D38
6262382D61653633306236636132653000000000
```

2

Rekey

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: 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: 964d3dd2-
5f06-4529-8bb8-ae630b6ca2e0
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F0100000048420
05C050000000400000004000000004200790100000030420094070000002439363464336464322D3566
30362D343532392D386262382D6165363330623663613265300000000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA
(Fri Apr 27 10:12:26 CEST 2012)
    Tag: 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: 3f190eed-
04b7-4220-80a4-fa18e28faaee
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A54EA42000D020000000400000
0001000000000042000F010000005842005C05000000040000000040000000042007F050000000040000000
000000000042007C010000003042009407000000024336631393065656 42D303462372D343232302D38
3061342D66613138653238666161656500000000
```

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: 
0x00000001 (1)
    Tag: 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)
```

```
42007801000000A0420077010000003842006901000000200420 06A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F0100000005842 00
5C050000000400000008000000000420079010000004042000801000000384 2000A070000000044E616D
65000000000042000B010000002042005507000000008726 56B65794B657942005405000000040000000 1
00000000
```

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: 0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA (Fri Apr 27 10:12:26 CEST 2012) Tag: 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: 3f190eed-04b7-4220-80a4-fa18e28faaee 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000001000000004200920900000008000000004F9A54EA42000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F0500000004000000000000000042007C01000000304200940700000024336631393065656642D303462372D343232302D383061342D66613138653238666161656500000000
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: 0x00000001 (1) Tag: 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: 964d3dd2-5f06-4529-8bb8-ae630b6ca2e0
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
```

```
42007801000000A042007701000000384200690100000020420006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000584200
5C0500000004000000B0000000042007901000000404200940700000024393634643364643222D3566
30362D343532392D386262382D616536333062366361326530000000000042000A07000000044E616D65
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: 0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA (Fri Apr 27 10:12:26 CEST 2012)
    Tag: 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: 964d3dd2-5f06-4529-8bb8-ae630b6ca2e0
```

```
42007B01000000B042007A01000000484200690100000020420006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A54EA42000D020000000040000
00010000000042000F01000000584200 5C0500000004000000B000000000042007F0500000004000000
0000000000042007C01000000304200940700000024393634643364643222D356630362D343532392D38
6262382D616536333062366361326530000000
```

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:
0x00000001 (1)
    Tag: 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: 964d3dd2-
5f06-4529-8bb8-ae630b6ca2e0
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000484200
5C05000000040000000A00000000420079010000003042009407000000243936346433646432 2D3566
30362D343532392D386262382D616536333062366361326530000000000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA
(Fri Apr 27 10:12:26 CEST 2012)
    Tag: 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: 964d3dd2-5f06-4529-8bb8-ae630b6ca2e0

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 9CA9840291A65889043C37707DA997E8

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

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

```
42007B01000001204200 7A01000000484200690100000020 42006A02000000040000000100000000 42
```

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: 0x00000001 (1)

    Tag: 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: 964d3dd2-
5f06-4529-8bb8-ae630b6ca2e0
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
5C0500000004000000140000000042007901000000304200940700000024393634643364643222D3566
30362D343532392D386262382D616536333062366361326530000000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA
(Fri Apr 27 10:12:26 CEST 2012)

    Tag: 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: 964d3dd2-
5f06-4529-8bb8-ae630b6ca2e0
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A54EA42000D0200000004000
0000100000000042000F010000005842005C0500000004000000140000000042007F0500000004000000
000000000042007C01000000304200940700000024393634643364643222D356630362D343532392D38
6262382D616536333062366361326530000000000
```

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: 
0x00000001 (1)
    Tag: 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: 3f190eed-
04b7-4220-80a4-fa18e28faaee
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000484200
5C05000000040000001400000000420079010000003042009407000000243366313930656564 2D3034
62372D343232302D383061342D66613138653238666161656500000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EA 
(Fri Apr 27 10:12:26 CEST 2012)
    Tag: 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: 3f190eed-04b7-4220-80a4-fa18e28faaee 42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042 006B02000000040000000100000000420092090000000800000004F9A54EA42000D02000000040000 0001000000000042000F01000000584200 5C05000000040000001400000000042007F0500000004000000 000000000042007C01000000304200940700000024336631393065656 42D303462372D343232302D38 3061342D666131386532386661616565000000000

9.2 Test Case: Existing Key Expired, Re-key with Same Life-cycle

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 the current time 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 Offset value of zero leading to the Activation Date of the replacement key to be set to the same value as the Initial Date of the replacement key. Verify from the response that the Activation Date and Deactivation Date attributes were set correctly (if they are not returned, issue a Get Attribute request). Do a Get Attribute operation to verify that the state of the new key is “Active”. To clean up, both keys are deleted.

Time	Request/Response messages
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:

```
0x00000001 (1)

    Tag: 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)
```

```
42007801000001604200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000001184200
5C050000000400000001000000004200790100000100420057050000000400000002000000000420091
01000000E84200080100000030 42000A070000001743727970746F67726170686963 20416C676F7269
74686D0042000B05000000040000000300000000420008010000003042000A07000000144372797074
6F67726170686963204C656E6774680000000042000B02000000040000008000000000420008010000
003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000
040000000C00000000420008010000003842000A07000000044E616D650000000042000B0100000020
420055070000000872656B65794B657942005405000000040000000100000000
```

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: 0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EB (Fri Apr 27 10:12:27 CEST 2012)
    Tag: 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: 5e2333ac-7cf2-402e-aa7a-0b6d1fd938cd
```

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A54EB42000D02000000040000
00010000000042000F010000006842005C0500000004000000010000000042007F0500000004000000
000000000042007C010000004042005705000000040000000200000000420094070000002435653233
333361632D376366322D343032652D616137612D30623664316664393338636400000000
```

1

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

In: uuidKey, attribute={ ActivationDate=’ <Timestamp in previous response>’ }

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: 
0x00000001 (1)

    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: Byte String (0x08), Data: 
606051F958D79B0F

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 5e2333ac-
7cf2-402e-aa7a-0b6d1fd938cd

      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: 
0x000000004F9A54EB (Fri Apr 27 10:12:27 CEST 2012)

  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: Byte String (0x08), Data: 
7CB12802F6A52CF1

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 5e2333ac-
7cf2-402e-aa7a-0b6d1fd938cd

      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: 
0x000000004F9A5563 (Fri Apr 27 10:14:27 CEST 2012)



42007801000001684200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000020000000042000F01000000884200
5C05000000040000000D000000004200930800000008606051F958D79B0F4200790100000060420094
070000002435653233333361632D376366322D343032652D616137612D306236643166643933386364
00000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B0900
000008000000004F9A54EB42000F010000009042005C05000000040000000D00000000420093080000
00087CB12802F6A52CF14200790100000068420094070000002435653233333361632D376366322D34
3032652D616137612D30623664316664393338636400000000420008010000003042000A0700000011
446561637469766174696F6E20446174650000000000000042000B0900000008000000004F9A5563
```

Out: uuidKey, attribute={ ActivationDate=’ <Timestamp in previous response>’ }

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: 0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EB (Fri Apr 27 10:12:27 CEST 2012)
    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: Byte String (0x08), Data: 606051F958D79B0F
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 5e2333ac-7cf2-402e-aa7a-0b6d1fd938cd
      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: 0x000000004F9A54EB (Fri Apr 27 10:12:27 CEST 2012)
  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: Byte String (0x08), Data: 7CB12802F6A52CF1
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 5e2333ac-7cf2-402e-aa7a-0b6d1fd938cd
      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:
0x000000004F9A5563 (Fri Apr 27 10:14:27 CEST 2012)



42007B010000019842007A010000004842006901000000204200 6A020000000400000001000000000042
```

```
42007B010000019842007A0100000048420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042009209000000080000000004F9A54EB42000D02000000040000
0002000000000042000F010000009842005C050000000400000000D000000004200930800000008606051
F958D79B0F42007F050000000400000000000000000042007C010000006042009407000000243565323 3
333361632D376366322D343032652D616137612D30623664316664393338636400000000420008010 0
00002842000A070000000F41637469766174696F6E204461746500420 00B09000000080000000004F9A
54EB42000F01000000A042005C050000000400000000D00000000420093080000000087CB12802F6A52C
F142007F05000000040000000000000000042007C010000006842009407000000243565323333336163
2D376366322D343032652D616137612D306236643166643933386364000000004200080100000003042
000A07000000114465616374697661746 96F6E204461746500000000000000042000B09000000080000
00004F9A5563
```

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:
0x00000001 (1)

    Tag: 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: 5e2333ac-
7cf2-402e-aa7a-0b6d1fd938cd

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



42007801000000A0420077010000003842006901000000204200 6A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F0100000058420 0
5C050000000400000000B000000004200790100000040420094070000002435653233333361632D3763
66322D343032652D616137612D306236643166643933386364000000000042000A070000000553746174
65000000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A54EB 
(Fri Apr 27 10:12:27 CEST 2012)

    Tag: 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: 5e2333ac-
7cf2-402e-aa7a-0b6d1fd938cd

      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)
```

```
42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A54EB42000D0200000004000
00001000000000042000F01000000080420050C0500000004000000B0000000042007F0500000004000000
000000000042007C010000005842009407000000243565323333361632D376366322D343032652D61
6137612D306236643166643933386364000000004200080100000002042000A070000000055374617465
00000042000B05000000040000000200000000
```

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:
0x00000001 (1)

    Tag: 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: 5e2333ac-
7cf2-402e-aa7a-0b6d1fd938cd

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

```
42007801000000A0420077010000003842006901000000204200 6A0200000004000000010000000042
```

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

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563
(Fri Apr 27 10:14:27 CEST 2012)

    Tag: 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: 5e2333ac-7cf2-402e-aa7a-0b6d1fd938cd 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) 42007B01000000D842007A0100000048420069010000002042006A02000000040000000100000000420 06B02000000040000000100000000420092090000000800000004F9A556342000D020000000400000 00010000000042000F010000008042005C0500000004000000B000000042007F05000000040000000 000000000042007C0100000058420094070000002435653233333361632D37636632D343032652D61 6137612D30623664316664393338636400000000420008010000002042000A07000000055374617465 00000042000B05000000040000000300000000
4	Rekey In: uuidKey, attribute={ offset='00000000' (set Activation Date and Initial Date of replacement key to the current time)} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: 5e2333ac-7cf2-402e-aa7a-0b6d1fd938cd Tag: Offset (0x420058), Type: Interval (0x0A), Data: 0x00000000 42007801000000A0420077010000003842006901000000204200 6A0200000004000000010000000042 006B0200000004000000010000000042000D0200000004000000010000000042000F01000000584200 5C05000000040000000400000000420079010000004042009407000000243565323333336163 2D3763 66322D343032652D616137612D30623664316664393338636400000000420058 0A000000040000000 00000000

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563
(Fri Apr 27 10:14:27 CEST 2012)
    Tag: 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: 8efbbd67-
2847-46b5-b7e7-4ab3b5e175de
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B020000000400000001000000004200920900000008000000004F9A556342000D02000000040000
00010000000042000F01000000058420005C05000000040000000400000000042007F050000000400000
0000000000042007C01000000304200940700000024386566626264363372D323834372D343662352D62
3765372D34616233623565313735646500000000
```

5

Get Attribute

In: uuidNewKey, attributeName={‘ ActivationDate’, ‘DectivationDate’ }

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

```
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: 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: 8efbbd67-
2847-46b5-b7e7-4ab3b5e175de

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

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

```
42007801000000C84200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000804200
5C05000000040000000B000000004200790100000068420094070000002438656662626436372D3238
34372D343662352D623765372D346162336235653137356465000000000042000A070000000F41637469
766174696F6E20446174650042000A0700000011446561637469766174696F6E2044617465000000000
000000
```

Out: uuidNewKey, attribute={ ActivationDate=' <Value of ActivationTime in existing key>', DectivationDate='<Value of DeactivationDate of existing key + <Difference between ActivationTime of Replacement and Replaced Key>>' }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563 
(Fri Apr 27 10:14:27 CEST 2012)

    Tag: 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: 8efbbd67-2847-46b5-b7e7-4ab3b5e175de

      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: 0x000000004F9A5563 (Fri Apr 27 10:14:27 CEST 2012)

      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: 0x000000004F9A55DB (Fri Apr 27 10:16:27 CEST 2012)
```

```
42007B010000011842007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000100000000420092090000000800000004F9A556342000D02000000040000000010000000042000F01000000C042005C05000000040000000B000000042007F0500000004000000000000000042007C0100000098420094070000002438656662626436372D323834372D343662352D623765372D34616233623565313735646500000000420008010000002842000A070000000F41637469766174696F6E20446174650042000B0900000008000000004F9A5563420008010000003042000A0700000011446561637469766174696F6E2044617465000000000000000042000B0900000008000000004F9A55DB
```

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: 0x00000001 (1)

    Tag: 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: 8efbbd67-
```

```
2847-46b5-b7e7-4ab3b5e175de

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


42007801000000A042007701000000384200690100000020420006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000584200
5C05000000040000000B00000000420079010000004042009407000000243865666262643637 2D3238
34372D343662352D623765372D346162336235653137356465000000000042000A070000000553746174
65000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563
(Fri Apr 27 10:14:27 CEST 2012)

    Tag: 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: 8efbbd67-
2847-46b5-b7e7-4ab3b5e175de

      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)


42007B01000000D842007A01000000484200690100000020420006A02000000040000000100000000042
006B02000000040000000100000000042009209000000080000000004F9A556342000D02000000040000
000100000000042000F010000008042005C05000000040000000B00000000042007F05000000004000000
00000000042007C010000005842009407000000243865666262643637 2D323834372D343662352D62
3765372D346162336235653137356465000000000420008010000002042000A07000000055374617465
00000042000B05000000040000000200000000
```

7 Destroy

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: 5e2333ac-
7cf2-402e-aa7a-0b6d1fd938cd
```

```
420078010000009042007701000000384200690100000020420006A02000000040000000100000000042
006B02000000004000000010000000042000D020000000400000001000000042000F01000000484200
5C0500000004000000140000000042007901000000304200940700000024356532333361632D3763
66322D343032652D616137612D30623664316664393338636400000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563 
(Fri Apr 27 10:14:27 CEST 2012)
```

```
    Tag: 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: 5e2333ac-
7cf2-402e-aa7a-0b6d1fd938cd



42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000000 4F9A556342000D02000000040000
00010000000042000F010000005842005C05000000040000001400000000042007F0500000004000000
000000000042007C0100000030420094070000002435653233333361632D376366322D343032652D61
6137612D30623664316664393338636400000000
```

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

In (header): batchOrderOption='TRUE'

In: uuidKey, revocationReasonCode='6'

In: uuidNewKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

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

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
955DFBB9ABBEC308

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 8efbbd67-
2847-46b5-b7e7-4ab3b5e175de

      Tag: Revocation Reason (0x420081), Type: Structure (0x01), Data:
        Tag: Revocation Reason Code (0x420082), Type: Enumeration (0x05), Data: 0x00000006 (Cessation of Operation)

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 6CE5EA0C8334B076

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 8efbbd67-2847-46b5-b7e7-4ab3b5e175de
```

```
42007801000001284200770100000048420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042001006000000080000000000000001420000D02000000040000
00020000000042000F01000000704200 5C0500000004000000130000000042009308000000008955DFB
B9ABBEC30842007901000000484200940700000024386566626264363 72D323834372D343662352D62
3765372D34616233623565313735646500000000420081010000001042008205000000040000000600
00000042000F01000000584200 5C050000000400000014000000004200930800000008 6CE5EA0C8334
B07642007901000000304200940700000024386566626264363 72D323834372D343662352D62376537
2D346162336235653137356465 00000000
```

Out: uuidNewKey

Out: uuidNewKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563 (Fri Apr 27 10:14:27 CEST 2012)

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 955DFBB9ABBEC308

    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 8efbbd67-
2847-46b5-b7e7-4ab3b5e175de
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014
(Destroy)
    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
6CE5EA0C8334B076
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000
(Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 8efbbd67-
2847-46b5-b7e7-4ab3b5e175de
```

```
42007B010000013042007A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A556342000D02000000040000
00020000000042000F010000006842005C050000000400000013000000004200930800000008955DFB
B9ABBEC30842007F0500000004000000000000000042007C0100000030420094070000002438656662
626436372D323834372D343662352D623765372D3461623362356531373564650000000042000F0100
00006842005C0500000004000000140000000042009308000000086CE5EA0C8334B07642007F050000
0004000000000000000042007C0100000030420094070000002438656662626436372D323834372D34
3662352D623765372D34616233623565313735646500000000
```

9.3 Test Case: Existing Key Compromised, Re-key with Same Life-cycle

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	Request/Response messages
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:
0x00000001 (1)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000002
(Symmetric Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data:
Cryptographic Algorithm
          Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data:
0x00000003 (AES)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data:
Cryptographic Length
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000080
(128)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data:
Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x0000000C
(Encrypt, Decrypt)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data:
Activation Date
          Tag: Attribute Value (0x42000B), Type: Date-Time (0x09), Data:
0x000000004F9A5563 (Fri Apr 27 10:14:27 CEST 2012)
        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)
```

```
42007801000001904200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000001484200
5C0500000004000000010000000042007901000001304200570500000004000000020000000420091
01000001184200080100000030420000A070000001743727970746F6772617068696320416C676F7269
74686D0042000B05000000040000000300000000420008010000003042000A0700000014437279707 4
6F6772617068696320C656E67746800000000042000B0200000004000000080000000042000801000 0
003042000A0700000018437279707 46F6772617068696320557361676520 4D61736B42000B02000000
040000000C00000000420008010000002842000A070000000F416374697661746 96F6E2044617465 00
42000B090000000080000000 04F9A5563420008010000003842000A07000000044E616D650000000042
000B01000000204200550700000008726 56B65794B6579420054050000000400000001000000 00
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563
(Fri Apr 27 10:14:27 CEST 2012)

    Tag: 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: 89860b8d-
a01e-43d0-a14d-0b1a15939af1
```

```
42007B01000000C042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000000 4F9A556342000D0200000004000 0
000100000000042000F01000000684200 5C0500000004000000010000000042007F0500000004000000
0000000000042007C0100000040420057050000000400000002000000004200940700000024383938 36
306238642D613031652D343364302D613134642D3062316131353933396166310000000 0
```

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: 
0x00000001 (1)
    Tag: 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: 89860b8d-
a01e-43d0-a14d-0b1a15939af1
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
```

```
42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000584200
5C0500000004000000B000000004200790100000040420094070000002438393836306238642D6130
31652D343364302D613134642D30623161313539333961663100000000042000A070000000553746174
65000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563 
(Fri Apr 27 10:14:27 CEST 2012)
    Tag: 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: 89860b8d-a01e-43d0-a14d-0b1a15939af1 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) 42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042 006B02000000040000000100000000420092090000000800000004F9A556342000D02000000040000 0001000000000042000F010000008042005C0500000004000000B000000000042007F0500000004000000 000000000042007C0100000058420094070000002438393836306238642D613031652D343364302D61 3134642D30623161313539333961663100000000420008010000002042000A070000000553746174 65 00000042000B05000000040000000200000000
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: 0x00000001 (1) Tag: 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: 89860b8d-a01e-43d0-a14d-0b1a15939af1 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: 
0x000000004F9A5563 (Fri Apr 27 10:14:27 CEST 2012)
```

```
42007801000000B84200770100000038420069010000002042006A02000000040000000100000000420
06B0200000004000000010000000042000D0200000004000000010000000042000F01000000704200
5C0500000004000000130000000042007901000000584200940700000024383938363062386420D6130
31652D343364302D613134642D306231613135393339616631000000004200810100000010420082050
00000040000000200000000420021090000000800000004F9A5563
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563 
(Fri Apr 27 10:14:27 CEST 2012)
    Tag: 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: 89860b8d-
a01e-43d0-a14d-0b1a15939af1
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420
06B020000000400000001000000004200920900000008000000004F9A556342000D020000000400000
00010000000042000F01000000584200 5C0500000004000000130000000042007F050000000400000000
00000000042007C010000003042009407000000243839383630623864 2D613031652D343364302D61
3134642D306231613135393339616631 00000000
```

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:
0x00000001 (1)
    Tag: 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: 89860b8d-
a01e-43d0-a14d-0b1a15939af1
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: State
```

```
42007801000000A0420077010000003842006901000000204200６A02000000040000000100000000042
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563
(Fri Apr 27 10:14:27 CEST 2012)
    Tag: 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: 89860b8d-a01e-43d0-a14d-0b1a15939af1 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) 42007B01000000D842007A0100000048420069010000002042006A02000000040000000100000000042 006B020000000400000001000000004200920900000008000000004F9A556342000D020000000400000 00010000000042000F01000000804200 5C050000000400000000B000000000042007F05000000004000000 00000000000042007C010000005842009407000000243839383630623864 2D613031652D343364302D61 3134642D30623161313539333961663100000000420008010000002042000A07000000055374617465 00000042000B05000000004000000040000000
4	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: 0x00000001 (1) Tag: 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: 89860b8d-a01e-43d0-a14d-0b1a15939af1 420078010000009042007701000000384200690100000020 42006A02000000040000000100000000042 006B02000000040000000100000000042000D02000000040000000100000000042000F010000004842 00 5C05000000040000000400000000420079010000003042009407000000243839383630623864 2D6130 31652D343364302D613134642D3062316131353933396166310000000 0

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563 
(Fri Apr 27 10:14:27 CEST 2012)
    Tag: 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: 7a89b8aa-
824d-4dc1-95e0-cac9b7b2e944
```

```
42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042
006B020000000400000001000000042009209000000080000000004F9A556342000D02000000040000
00010000000042000F010000005842005C050000000400000004000000042007F0500000004000000
0000000000042007C0100000030420094070000002437613839623861612D383234642D346463312D39
3565302D63616339623762326539343400000000
```

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: 
0x00000001 (1)
```

```
    Tag: 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: 7a89b8aa-
824d-4dc1-95e0-cac9b7b2e944

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

```
42007801000000A04200770100000038420069010000002042006A020000000400000001000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000584200
5C0500000004000000B00000000420079010000004042009407000000243761383962386161 2D3832
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563
(Fri Apr 27 10:14:27 CEST 2012)

    Tag: 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: 7a89b8aa-
824d-4dc1-95e0-cac9b7b2e944

      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)
```

```
42007B01000000D842007A0100000048420069010000002042006A02000000040000000100000000420
06B02000000040000000100000000420092090000000800000004F9A556342000D020000000400000
00100000000042000F010000008042005C0500000004000000B000000000042007F05000000040000000
00000000042007C0100000058420094070000002437613839623861612D383234642D346463312D39
3565302D63616339623762326539343400000000420008010000002042000A07000000055374617465
00000042000B050000000400000000200000000
```

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:
0x00000001 (1)
    Tag: 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: 89860b8d-
a01e-43d0-a14d-0b1a15939af1
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000420
06B02000000040000000100000000042000D02000000040000000100000000042000F0100000048420
05C05000000040000001400000000420079010000003042009407000000243839383630623864D6130
31652D343364302D613134642D306231613135393339616631000000000
```

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: 0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563 (Fri Apr 27 10:14:27 CEST 2012) Tag: 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: 89860b8d-a01e-43d0-a14d-0b1a15939af1 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042 006B020000000400000001000000004200920900000008000000004F9A556342000D020000000400000 0001000000042000F010000005842005C050000000400000014000000042007F050000000400000 000000000042007C01000000304200940700000024383938363062386442D613031652D343364302D61 3134642D30623161313539333961663100000000
7	Revoke (symmetric key as cessation of operation) and Destroy In (header): batchOrderOption='TRUE' In: uuidNewKey, revocationReasonCode='6' In: uuidNewKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
C95BBFD6AD466474

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 7a89b8aa-
824d-4dc1-95e0-cac9b7b2e944

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

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
4E6A3E943E1DDA87

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 7a89b8aa-
824d-4dc1-95e0-cac9b7b2e944
```

```
42007801000001284200770100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420010060000000800000000000000014200 0D02000000040000
```

Out: uuidNewKey

Out: uuidNewKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563
(Fri Apr 27 10:14:27 CEST 2012)
```

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
C95BBFD6AD466474

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 7a89b8aa-
824d-4dc1-95e0-cac9b7b2e944

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
4E6A3E943E1DDA87

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 7a89b8aa-
824d-4dc1-95e0-cac9b7b2e944



42007B010000013042007A0100000048420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042009209000000080000000004F9A556342000D020000000400000
0002000000000042000F01000000068420005C05000000040000001300000000420093080000008C95BBF
D6AD46647442007F0500000004000000000000000042007C01000000304200940700000024376138 39
623861612D383234642D346463312D393565302D63616339623762326539343400000000042000F0100
00006842005C0500000004000000140000000042009308000000084E6A3E943E1DDA8742007F050000
0004000000000000000042007C010000003042009407000000243761383962386161 2D383234642D34
6463312D393565302D636163396237623265393434000000000
```

9.4 Test Case: Create Key, Re-key with New Life-cycle

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

Time	Request/Response messages
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: 0x00000001 (1)
    Tag: 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)
```

```
42007801000001604200770100000038420069010000002042006A0200000004000000010000000042
```

```
006B02000000040000000100000000042000D0200000004000000010000000042000F01000001184200
5C050000000400000001000000004200790100000100420057050000000400000002000000000420091
01000000E842000801000000303042000A070000001743727970746F677261706869632041 6C676F7269
```

```
006B02000000040000000100000000042000D0200000004000000010000000042000F01000001184200
5C05000000040000000100000000420079010000010042005705000000040000000200000000420091
01000000E8420008010000003042000A070000001743727970746F6772617068696320416C676F7269
74686D0042000B05000000040000000300000000420008010000003042000A0700000014437279707 4
6F6772617068696320 4C656E677468000000042000B020000000400000080000000004200080100000
003042000A0700000018437279707 46F677261706869632055736167652 04D61736B42000B02000000
040000000C00000000420008010000003842000A07000000044E616D65000000042000B0100000020
4200550700000008 72656B65794B6579420054050000000400000001 00000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563 
(Fri Apr 27 10:14:27 CEST 2012)
    Tag: 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: 1346d253-
69d6-474c-8cd5-ad475a3e0a81
```

```
42007B01000000C042007A0100000048420069010000002042006A020000000400000001000000042
006B02000000040000000100000000420092090000000800000004F9A556342000D020000000400000
00010000000042000F010000006842005C0500000004000000010000000042007F050000000400000
00000000000042007C010000004042005705000000040000000200000000420094070000002431333436
643235332D363964362D343734632D386364352D616434373561336530613831 00000000
```

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: 
0x00000001 (1)
    Tag: 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)
```

```
42007801000000A04200770100000038420069010000002042006A02000000040000000100000000 42
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000584200
5C0500000004000000080000000042007901000000404200080100000038420000A07000000044E616D
650000000042000B01000000204200550700000008 72656B65794B65794200540500000004000000001
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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563 
(Fri Apr 27 10:14:27 CEST 2012)
```

	Tag: 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: 1346d253-69d6-474c-8cd5-ad475a3e0a81 42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420 06B02000000040000000100000000420092090000000800000004F9A556342000D0200000004000000010000000042000F010000005842005C050000000400000008000000042007F05000000040000000000000000042007C0100000030420094070000002431333436643235332D363964362D343734632D386364352D6164343735613365306138310000000 0
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: 0x00000001 (1) Tag: 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: 1346d253-69d6-474c-8cd5-ad475a3e0a81 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 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)
```

```
42007801000001704200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000001284200
5C0500000004000000040000000042007901000001104200940700000024313334366432353332D3639
64362D343734632D386364352D61643437356133653061383100000000420091010000000D842000801
0000002842000A070000000F416374697661746696F6E204461746500420000B0900000008000000043
B7B63042000801000000303042000A07000000125072656F6365737320537461727420446174650000000
000042000B09000000080000000043B7B63042000801000000303042000A07000000115072656F74656374
2053746F7020446174650000000000000042000B09000000080000000005E0C7BB042000801000000030
42000A07000000114465616374697661746696F6E204461746500000000000000042000B090000000800
0000005E0C7BB0
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563
(Fri Apr 27 10:14:27 CEST 2012)

    Tag: 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: 6766f95e-
740f-4b4d-aa55-97c3f4f19dd5


42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000004F9A556342000D02000000040000
00010000000042000F01000000584200 5C050000000400000004000000000042007F0500000004000000
000000000042007C0100000030420094070000002436373636663935652D373430662D346234642D61
6135352D39376333663466313964643500000000
```

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:
0x00000001 (1)
    Tag: 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: 1346d253-
69d6-474c-8cd5-ad475a3e0a81
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name


42007801000000A042007701000000384200690100000020420006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000584200
5C0500000004000000 0B000000004200790100000040420094070000002431333436643235332D3639
64362D343734632D386364352D616434373561336530613831000000000042000A07000000044E616D65
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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5563 
(Fri Apr 27 10:14:27 CEST 2012)
    Tag: 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: 1346d253-
69d6-474c-8cd5-ad475a3e0a81
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A556342000D02000000040000
0001000000000042000F010000005842005C05000000040000000B000000000042007F0500000004000000
00000000000042007C0100000030420094070000002431333436643235332D363964362D343734632D38
6364352D616434373561336530613831000000000
```

4

Get Attribute

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

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

```
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: 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: 6766f95e-
740f-4b4d-aa55-97c3f4f19dd5

      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
```

```
42007801000001084200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000C04200
5C05000000040000000B00000000420079010000000A84200940700000024363736366663935652D3734
30662D346234642D616135352D39376333663466313964643500000000042000A070000000F41637469
766174696F6E20446174650042000A070000001250726F63657373205374617274204461746500000000
00000042000A070000001150726F746563742053746F70204461746500000000000000042000A070000
00114465616374697661746696F6E2044617465000000000000000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564 
(Fri Apr 27 10:14:28 CEST 2012)

    Tag: 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: 6766f95e-
740f-4b4d-aa55-97c3f4f19dd5

      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)



42007B01000001884200 7A0100000048420069010000002042006A0200000004000000010000000042
```

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:
0x00000001 (1)
    Tag: 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)
```

```
42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000584200
5C05000000040000000800000000420079010000004042000801000000038420000A07000000044E616D
65000000000042000B01000000204200550700000000872656B65794B65794200540500000000400000001
00000000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564
(Fri Apr 27 10:14:28 CEST 2012)
    Tag: 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: 6766f95e-740f-4b4d-aa55-97c3f4f19dd5 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042 006B02000000040000000100000000420092090000000800000004F9A556442000D020000000400000 0001000000000042000F010000005842005C0500000004000000080000000042007F0500000004000000 000000000042007C010000003042009407000000243637366663935652D373430662D346234642D61 6135352D393763336634663139646435000000000
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: 0x00000001 (1) Tag: 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: 1346d253-69d6-474c-8cd5-ad475a3e0a81 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042 006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200 5C050000000400000014000000004200790100000030420094070000002431333436643235332D3639 64362D343734632D386364352D616434373561336530613831000000000 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: 0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564 (Fri Apr 27 10:14:28 CEST 2012)
    Tag: 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: 1346d253-69d6-474c-8cd5-ad475a3e0a81
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A556442000D02000000040000
00010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000
000000000042007C0100000030420094070000002431333436643235332D363964362D343734632D38
6364352D61643437356133653061383100000000
```

7

Revoke (symmetric key as cessation of operation) and Destroy

In (header): batchOrderOption='TRUE'

In: uuidNewKey, revocationReasonCode='6'

In: uuidNewKey

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

```
0x00000001 (1)

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

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

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
64BF984D81EEE045

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6766f95e-
740f-4b4d-aa55-97c3f4f19dd5

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

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
6E140354775E324D

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6766f95e-
740f-4b4d-aa55-97c3f4f19dd5
```

```
42007801000001284200770100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420010060000000800000000000000014200 0D02000000040000
0002000000042000F010000007042005C0500000004000000130000000042009308000000864BF98
4D81EEE045420079010000004842009407000000243637363666393565 2D373430662D346234642D61
6135352D39376333663466313964643500000000420081010000001042008205000000040000000600
000000 42000F010000005842005C05000000040000001400000000420093080000000 86E140354775E
324D4200790100000030420094070000002436373636663935652D373430662D346234642D61613535
2D39376333663466313964643500000000
```

Out: uuidNewKey

Out: uuidNewKey

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564 
(Fri Apr 27 10:14:28 CEST 2012)

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
64BF984D81EEE045

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6766f95e-
740f-4b4d-aa55-97c3f4f19dd5

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
6E140354775E324D

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 6766f95e-
740f-4b4d-aa55-97c3f4f19dd5



42007B010000013042007A0100000048420069010000002042006A020000000400000001000000000042
006B0200000004000000010000000042009209000000080000000004F9A556442000D02000000040000
00020000000042000F010000006842005C050000000400000013000000004200930800000000864BF98
4D81EEE04542007F0500000004000000000000000042007C0100000030420094070000002436373636
663935652D373430662D346234642D616135352D3937633366346631396464350000000042000F0100
00006842005C05000000040000001400000000420093080000000086E140354775E324D42007F050000
00040000000000000000042007C01000000304200940700000024363736366639356 52D373430662D34
6234642D616135352D39376333663466313964643500000000
```

9.5 Test 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 due to a server policy which does not allow giving out leases for compromised keys. Locate the new key with the original name. Get the new key and obtain a lease.

Time	Request/Response messages
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:
0x00000001 (1)
    Tag: 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)

        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:
0x000000004F9A5564 (Fri Apr 27 10:14:28 CEST 2012)
```

```
42007801000001904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000001484200
5C05000000040000000100000000420079010000013042005705000000040000000200000000420091
0100000118420008010000003042000A070000001743727970746F6772617068696320416C676F7269
74686D0042000B05000000040000000300000000420008010000003042000A07000000144372797074
6F6772617068696320C656E6774680000000042000B02000000040000000800000000420008010000
003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000
040000000C00000000420008010000003842000A07000000044E616D650000000042000B0100000020
42005507000000087265 6B65794B657942005405000000040000000100000000420008010000002842
000A070000000F4163746976617469 6F6E20446174650042000B09000000080000000004F9A5564
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564
(Fri Apr 27 10:14:28 CEST 2012)

    Tag: 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: f4152f17-
9312-431a-b3fb-4fe86a86a7a1
```

```
42007B01000000C042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A556442000D0200000004000000
00010000000042000F010000006842005C05000000040000000100000000042007F05000000040000000
00000000042007C010000004042005705000000040000000200000000420094070000002466343135
326631372D393331322D343331612D623366622D34666538366138366137613100000000
```

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:
0x00000001 (1)

    Tag: 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: f4152f17-
9312-431a-b3fb-4fe86a86a7a1
```

```
420078010000009042007701000000384200690100000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000484200
5C05000000040000000A0000000042007901000000304200940700000024663431353266631372D3933
31322D343331612D623366622D34666538366138366137613100000000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564 
(Fri Apr 27 10:14:28 CEST 2012)

    Tag: 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: f4152f17-
9312-431a-b3fb-4fe86a86a7a1

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 
EF5A0E97A29B32034C66EFBF26AD3E42

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

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



42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A556442000D02000000040000
00010000000042000F01000000C842005C05000000040000000A0000000042007F0500000004000000
000000000042007C01000000A04200570500000004000000020000000042009407000000246634313 5
326631372D393331322D343331612D623366622D3466653836613836613761310000000042008F0100
0000584200400100000050420042050000000400000001000000004200450100000018420043080000
0010EF5A0E97A29B32034C66EFBF26AD3E424200280500000004000000030000000042002A02000000
040000008000000000
```

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: 
0x00000001 (1)
    Tag: 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: f4152f17-
9312-431a-b3fb-4fe86a86a7a1
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F010000004842000
5C05000000040000001000000000420079010000003042009407000000246634313532663137 2D3933
31322D343331612D623366622D34666538366138366137613100000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564 
(Fri Apr 27 10:14:28 CEST 2012)
    Tag: 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: f4152f17-9312-431a-b3fb-4fe86a86a7a1
      Tag: Lease Time (0x420049), Type: Interval (0x0A), Data: 0x00000000
      Tag: Last Change Date (0x420048), Type: Date-Time (0x09), Data: 0x000000004F9A5564 (Fri Apr 27 10:14:28 CEST 2012)
```

```
42007B01000000D042007A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A556442000D02000000040000
00010000000042000F010000007842005C0500000004000000100000000042007F0500000004000000
000000000042007C0100000050420094070000002466343135326631372D393331322D343331612D62
3366622D346665383661383661376131000000004200490A0000000400000000000000004200480900
000008000000004F9A5564
```

3 Client B:

Revoke (symmetric key as compromised)

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

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
    Tag: 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: f4152f17-9312-431a-b3fb-4fe86a86a7a1
      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: 
0x000000004F9A5564 (Fri Apr 27 10:14:28 CEST 2012)
```

```
42007801000000B84200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000704200
5C05000000040000001300000000420079010000005842009407000000246634313532663137 2D3933
31322D343331612D623366622D34666538366138366137613100000000420081010000001042008205
00000004000000020000000042002109000000080000000004F9A5564
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564 
(Fri Apr 27 10:14:28 CEST 2012)
    Tag: 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: f4152f17-
9312-431a-b3fb-4fe86a86a7a1
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B020000000400000001000000004200920900000008000000004F9A556442000D02000000040000
00010000000042000F010000005842005C05000000040000001300000000042007F050000000400000
000000000042007C010000003042009407000000246634313532663137 2D393331322D343331612D62
3366622D346665383661383661376131 00000000
```

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:
0x00000001 (1)
    Tag: 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: f4152f17-
9312-431a-b3fb-4fe86a86a7a1
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C050000000400000004000000004200790100000030420094070000002466343135326631372D3933
31322D343331612D623366622D34666538366138366137613100000000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564
(Fri Apr 27 10:14:28 CEST 2012)
    Tag: 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: 28a84544-7c4a-4d48-8e71-07f5b000663e
	
	42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420006B0200000004000000010000000042009209000000080000000004F9A556442000D0200000004000000001000000000042000F01000000058420005C05000000040000000040000000042007F0500000000400000000000000000042007C010000003042009407000000024323861383435343442D376334612D346434382D386537312D3037663562303030363633650000000000

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: 0x00000001 (1)
	    Tag: 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: f4152f17-9312-431a-b3fb-4fe86a86a7a1
	
	420078010000009042007701000000384200690100000020042006A020000000400000001000000000042006B020000000400000001000000000042000D02000000040000000100000000042000F010000004842005C050000000400000010000000000420079010000003042009407000000024663431353266313732D393331322D343331612D623366622D34666538366138366137613100000000
	
	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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564
(Fri Apr 27 10:14:28 CEST 2012)

    Tag: 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


42007B01000000C042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A556442000D020000000040000
0001000000000042000F01000000068420005C0500000004000000100000000042007F0500000004000000
0100000000042007E050000000400000000C0000000042007D070000002A434F20697320696E20737461
746520436F6D70726F6D697365642C206E6F206C656173652067697656E000000000000
```

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:
0x00000001 (1)
```

```
    Tag: 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)
```

```
42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420000D0200000004000000010000000042000F01000000584200
5C0500000004000000080000000042007901000000404200080100000038420000A07000000044E616D
650000000042000B010000002042005507000000087265 6B65794B65794200540500000004000000001
00000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564
(Fri Apr 27 10:14:28 CEST 2012)

    Tag: 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: 28a84544-
7c4a-4d48-8e71-07f5b000663e
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A556442000D02000000040000
00010000000042000F01000000584200 5C05000000040000000800000000042007F0500000004000000
00000000042007C010000003042009407000000243238613834353434 2D376334612D346434382D38
6537312D303766356230303036363365000000000
```

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:
0x00000001 (1)
    Tag: 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: 28a84544-
7c4a-4d48-8e71-07f5b000663e
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C0500000004000000A0000000042007901000000304200940700000024323861383435343 42D3763
34612D346434382D386537312D303766356230303036363365000000000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564 
(Fri Apr 27 10:14:28 CEST 2012)

    Tag: 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: 28a84544-
7c4a-4d48-8e71-07f5b000663e

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 
525D4B0BBB66BCB538029D49A6F569A5

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

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

```
42007B01000001204200 7A0100000048420069010000002042006A02000000040000000100000000042
```

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: 
0x00000001 (1)
    Tag: 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: 28a84544-
7c4a-4d48-8e71-07f5b000663e
```

```
4200780100000090420077010000003842006901000000204200６A02000000040000000100000000042
```

Out: uuidNewKey, leaseTime, lastChangeDate

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564 
(Fri Apr 27 10:14:28 CEST 2012)
    Tag: 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: 28a84544-7c4a-4d48-8e71-07f5b000663e Tag: Lease Time (0x420049), Type: Interval (0x0A), Data: 0x00000000 Tag: Last Change Date (0x420048), Type: Date-Time (0x09), Data: 0x000000004F9A5564 (Fri Apr 27 10:14:28 CEST 2012) 42007B01000000D042007A0100000048420069010000002042006A02000000040000000100000000042006B020000000400000001000000004200920900000008000000004F9A556442000D0200000004000000010000000042000F010000007842005C050000000400000001000000000042007F05000000040000000000000000042007C0100000050420094070000002432386138343534342D376334612D346434382D386537312D3037663562303030363633650000000042004 90A00000004000000000000000042004809000000008000000004F9A5564
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: 0x00000001 (1) Tag: 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: f4152f17-9312-431a-b3fb-4fe86a86a7a1 42007801000000904200770100000038420069010000002042006A02000000040000000100000000042006B020000000400000001000000000042000D020000000400000001000000000042000F010000004842005C05000000040000001400000000420079010000003042009407000000246634313532663137 2D393331322D343331612D623366622D34666538366138366137613100000000 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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564 
(Fri Apr 27 10:14:28 CEST 2012)
    Tag: 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: f4152f17-
9312-431a-b3fb-4fe86a86a7a1
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A556442000D020000000400000
00010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000
000000000042007C010000003042009407000000246634313532663137 2D393331322D343331612D62
3366622D3466653836613836613761310000000
```

10

Client A:

Revoke (symmetric key as cessation of operation) and Destroy

In (header): batchOrderOption='TRUE'

In: uuidNewKey, revocationReasonCode='6'

In: uuidNewKey

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)

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

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: E00004346EA64DA4

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 28a84544-7c4a-4d48-8e71-07f5b000663e

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

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 0376CA8CDCC8A2F1

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 28a84544-7c4a-4d48-8e71-07f5b000663e
```

```
42007801000001284200770100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420010060000000800000000000000014200 0D020000000400000
```

```
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564
(Fri Apr 27 10:14:28 CEST 2012)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000002 (2)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000013 (Revoke)
    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
E00004346EA64DA4
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000
(Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 28a84544-
7c4a-4d48-8e71-07f5b000663e
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014
(Destroy)
    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
0376CA8CDCC8A2F1
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000
(Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 28a84544-
7c4a-4d48-8e71-07f5b000663e
```

```
42007B010000013042007A0100000048420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042009209000000080000000004F9A556442000D0200000004000000
0002000000000042000F010000006842005C0500000004000000130000000042009308000000008E00004
346EA64DA442007F0500000004000000000000000042007C010000003042009407000000243238613 8
343534342D376334612D346434382D386537312D30376635623030303636336500000000042000F0100
00006842005C0500000004000000140000000042009308000000080376CA8CDCC8A2F142007F050000
00040000000000000000042007C01000000304200940700000024323861383435343 42D376334612D34
6434382D386537312D303766356230303036363365000000000
```

10 Archival

These test 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 Test Case: Create a Key, Archive and Recover it

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

Time	Request/Response messages

0	Create (symmetric key)
	In: objectType='00000002', attributes={ CryptographicAlgorithm='AES', CryptographicLength='128', CryptographicUsageMask='0000000C', 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: 0x00000001 (1)
	    Tag: 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: archiveKey
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 
(Uninterpreted Text String)
```

```
42007801000001684200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000001204200
5C05000000040000000100000000420079010000010842005705000000040000000200000000420091
01000000F04200080100000030420000A070000001743727970746F6772617068696320416C676F7269
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564
```

```
(Fri Apr 27 10:14:28 CEST 2012)

    Tag: 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: f613dba1-b557-489a-87c5-3c0ecd4294e3



42007B01000000C042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A556442000D020000000040000
00010000000042000F01000000684200 5C0500000004000000010000000042007F0500000004000000
0000000000042007C01000000404200570500000004000000020000000042009407000000246636313 3
646261312D623535372D343839612D383763352D33633065636434323934653300000000
```

1

Locate

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

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)

    Tag: 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) 42007801000000D84200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000010000000042000D0200000004000000010000000042000F010000009042005C05000000040000000800000000420079010000007842000801000000284200 0A070000000B4F626A656374205479706500000000000042000B05000000040000000200000000420008010000004042000A070000000 44E616D650000000042000B010000002842005507000000 0A617263686976654B6579000000000000042005405000000040000000100000000 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: 0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564 (Fri Apr 27 10:14:28 CEST 2012) Tag: 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: f613dba1-b557-489a-87c5-3c0ecd4294e3 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B020000000400000001000000004200920900000008000000004F9A556442000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F0500000004000000000000000042007C0100000030420094070000002466363133646261312D623535372D343839612D383763352D3363306563643432393465330000000
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: 
0x00000001 (1)

    Tag: 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: f613dba1-
b557-489a-87c5-3c0ecd4294e3
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000000A00000000420079010000003042009407000000246636313364626131 2D6235
35372D343839612D383763352D3363306563643432393465330000000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564 
(Fri Apr 27 10:14:28 CEST 2012)

    Tag: 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: f613dba1-b557-489a-87c5-3c0ecd4294e3
      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 (Raw)
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 0B4C9FB659C5CE09EC12C3233D526F45
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
```

```
42007B010000012042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A556442000D020000000400000
00010000000042000F01000000C842005C0500000004000000A00000000042007F050000000040000000
000000000042007C01000000A04200570500000004000000020000000042009407000000246636313 3
646261312D623535372D343839612D383763352D336330656364343239346533000000000042008F0100
0000584200400100000050420042050000000400000001000000004200450100000018420043080000
00100B4C9FB659C5CE09EC12C3233D526F454200280500000004000000030000000042002A02000000
040000008000000000
```

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: 0x00000001 (1)
    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: f613dba1-
b557-489a-87c5-3c0ecd4294e3
```

```
42007801000000A04200770100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420007060000000800000000000000142000D02000000040000
0001000000042000F01000000484200 5C05000000040000001500000000420079010000003042009 4
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5564
(Fri Apr 27 10:14:28 CEST 2012)

    Tag: 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: Byte String (0x08),
Data: 96A4660AED020302
```

```
42007B010000008842007A0100000048420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042009209000000080000000004F9A556442000D02000000040000
0001000000042000F01000000304 2005C05000000040000001500000000 42007F0500000004000000
0200000000420006080000000896A4660AED020302
```

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:
0x00000001 (1)
    Tag: 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: Byte String (0x08),
Data: 96A4660AED020302
```

```
42007801000000704200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000284200
5C05000000040000001A000000004200790100000010420006080000000896A4660AED020302
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5566
(Fri Apr 27 10:14:30 CEST 2012)
    Tag: 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: f613dba1-
b557-489a-87c5-3c0ecd4294e3
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A556642000D020000000400000
0001000000000042000F010000005842005C050000000400000015000000000042007F050000000400000
00000000000042007C01000000304200940700000024663631336462613132D623535372D343839612D38
3763352D3336333065636434323934653300000000
```

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:
0x00000001 (1)

    Tag: 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: f613dba1-
b557-489a-87c5-3c0ecd4294e3
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000000A00000000420079010000003042009407000000246636313336462613132D6235
35372D343839612D383763352D3336333065636434323934653300000000
```

Out: Operation Failed, Object Archived

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5568 
(Fri Apr 27 10:14:32 CEST 2012)
    Tag: 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


42007B01000000A842007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A556842000D02000000040000
00010000000042000F010000005042005C0500000004000000A0000000042007F0500000004000000
010000000042007E0500000004000000D0000000042007D07000000124F626A656374206973206172
63686976656400000000000000
```

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: 
0x00000001 (1)
    Tag: 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: f613dba1-
b557-489a-87c5-3c0ecd4294e3

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



42007801000000A84200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000604200
5C05000000040000000B00000000420079010000004842009407000000246636313364626131 2D6235
35372D343839612D383763352D336330656364343239346533000000000042000A070000000C41726368
6976652044617465000000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5568
(Fri Apr 27 10:14:32 CEST 2012)

    Tag: 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: f613dba1-
b557-489a-87c5-3c0ecd4294e3

      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:
0x000000004F9A5566 (Fri Apr 27 10:14:30 CEST 2012)



42007B01000000E042007A0100000048420069010000002042006A02000000040000000100000000042
```

```
006B020000000040000000010000000042009209000000008000000004F9A556842000D02000000040000
0001000000000042000F01000000088420005C0500000000400000000B0000000042007F0500000000400000
000000000042007C010000006042009407000000246636313364626131 2D623535372D343839612D38
3763352D33633065636434323934653300000000420008010000002842000A070000000C4172636869
766520446174650000000042000B09000000008000000004F9A5566
```

7

Locate

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

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

```
42007801000000D84200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000904200
5C050000000400000008000000004200790100000078420008010000002842000A070000000B4F626A
656374205479706500000000042000B05000000040000000200000000420008010000004042000A07
000000044E616D650000000042000B010000002842005507000000 0A617263686976654B6579000000
000000420054050000000400000001000000000
```

Out: <empty response payload>

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5569
(Fri Apr 27 10:14:33 CEST 2012)
    Tag: 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
```

```
42007B010000008042007A0100000048420069010000002042006A020000000400000001000000000042
006B02000000040000000100000000420092090000000800000004F9A556942000D020000000040000
0001000000000042000F010000002842005C0500000004000000080000000042007F0500000004000000
000000000042007C0100000000
```

8

Locate

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

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

```
42007801000000E84200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000A04200
5C050000000400000008000000004200790100000088420008E02000000040000000300000000420008
0100000028420000A070000000B4F626A656374205479706500000000000042000B050000000400000002
000000004200080100000040420000A07000000044E616D650000000042000B0100000028420055070 0
00000A617263686976654B65790000000000004200540500000004000000010000000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5569 
(Fri Apr 27 10:14:33 CEST 2012)
    Tag: 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: f613dba1-b557-489a-87c5-3c0ecd4294e3 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000100000000420092090000000800000004F9A556942000D0200000004000000010000000042000F010000005842005C0500000004000000080000000042007F0500000004000000000000000042007C010000003042009407000000246636313364626131 2D623535372D343839612D383763352D336330656364343239346533 00000000
9	Recover In: uuidKey, asynchronousIndicator='true' Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) 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: f613dba1-b557-489a-87c5-3c0ecd4294e3 42007801000000A0420077010000004842006901000000 2042006A0200000004000000010000000042006B0200000004000000010000000042000706000000080000000000000001 42000D0200000004000000010000000042000F010000004842005C050000000400000016000000004200790100000030420094070000002466363133646261312D623535372D343839612D383763352D33633065636434323934653300000000 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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5569 
(Fri Apr 27 10:14:33 CEST 2012)
    Tag: 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: Byte String (0x08), 
Data: E7125DE85B3C90A6
```

```
42007B01000000088420007A0100000048420069010000002042006A0200000004000000010000000042
```

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: 
0x00000001 (1)
    Tag: 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: Byte String (0x08),
Data: E7125DE85B3C90A6
```

```
42007801000000704200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000284200
5C0500000004000001A000000004200790100000010420006080000008E7125DE85B3C90A6
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B
(Fri Apr 27 10:14:35 CEST 2012)

    Tag: 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: f613dba1-
b557-489a-87c5-3c0ecd4294e3
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A556B42000D020000000040000
00010000000042000F01000000584200 5C05000000040000001600000000042007F050000000040000000
0000000042007C0100000030420094070000002466363133646261312D623535372D343839612D38
3763352D33633065636434323934653300000000
```

11 Get (symmetric key)

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
    Tag: 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: f613dba1-b557-489a-87c5-3c0ecd4294e3
```

```
420078010000009042007701000000384200690100000020420006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000484200
5C05000000040000000A00000000420079010000003042009407000000246636313364626131 2D6235
35372D343839612D383763352D336330656364343239346533 00000000
```

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: 0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B (Fri Apr 27 10:14:35 CEST 2012)
    Tag: 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: f613dba1-b557-489a-87c5-3c0ecd4294e3
      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 (Raw)
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 0B4C9FB659C5CE09EC12C3233D526F45
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
```

```
42007B01000001204200 7A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A556B42000D0200000004000000
0001000000000042000F01000000C842005C0500000004000000000A0000000042007F05000000040000000
000000000042007C01000000A04200570500000004000000002000000004200940700000024663631 33
646261312D623535372D343839612D383763352D336330656364343239346533000000000042008F0100
000058420040010000005042004205000000040000000100000000420045010000001842004308000000
00100B4C9FB659C5CE09EC12C3233D526F4542002805000000040000000300000000 42002A02000000
0400000008000000000
```

12

Destroy

In: uuidKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
    Tag: 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: f613dba1-
b557-489a-87c5-3c0ecd4294e3
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F0100000048 4200
5C0500000004000000140000000042007901000000304200940700000024663631336462613 12D6235
35372D343839612D383763352D33633065636434323934653300000000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B 
(Fri Apr 27 10:14:35 CEST 2012)

    Tag: 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: f613dba1-
b557-489a-87c5-3c0ecd4294e3
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000000 4F9A556B42000D02000000040000
00010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000
000000000042007C0100000030420094070000002466363133646261312D623535372D343839612D38
3763352D33633065636434323934653300000000
```

11 Access Control, Policies

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

11.1 Test Case: Credential, Operation Policy, Destroy Date

Pass a Credential object of type Username and Password in the message header in all requests for identification purposes (how the Credential object is used is defined in [KMIP-Spec]

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof]). Create a symmetric key and set the Operation Policy Name attribute to “default”. Using another Username and Password Credential, attempt to perform a Get operation batched with a Get Attribute List on the created symmetric key – according to the Default Operation Policy, both these request SHALL fail, and with the Batch Error Continuation Option set to “Continue”, the client SHALL also receive both response payloads. Using the initially used Credential, destroy the object and get the Destroy Date attribute.

The message exchanges in this test case are based on a certain server policy (e.g. handling of Credentials) that in some aspects differs from the policy assumed in earlier test cases (e.g. in this test case, the Destroy Date is retained). The message exchanges shown in this test case assume that both Credentials used in this example are for valid users of the server. As mentioned in Section 1 , the message exchanges shown in this document are not the only correct alternatives.

Time	Request/Response messages

0	Create (symmetric key)
	In (header): credential={ credentialType=’1’, credentialValue={ username=”Fred”, password=”password1” } }
	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: 0x00000001 (1)
    Tag: Authentication (0x42000C), Type: Structure (0x01), Data:
      Tag: Credential (0x420023), Type: Structure (0x01), Data:
        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password)
        Tag: Credential Value (0x420025), Type: Structure (0x01), Data:
          Tag: Username (0x420099), Type: Text String (0x07), Data: Fred
          Tag: Password (0x4200A1), Type: Text String (0x07), Data: password1
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 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-1335514339826
            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)
```

```
42007801000002584200770100000088420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000C010000004842002301000000404200240500000000040000
0001000000004200250100000028420099070000000446726564000000004200A10700000009706173
73776F72643100000000000000042000D020000000400000001000000000042000F01000001C042005C05
00000004000000010000000042007901000001A8420057050000000400000002000000004200910100
00019042000801000000030420000A070000000174372797074 6F677261706869632041 6C676F72697468
```

```
42007801000002584200770100000088420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000C0100000048420023010000004042002405000000040000
0001000000004200250100000028420099070000000446726564000000004200A10700000009706173
73776F726431000000000000000042000D0200000004000000010000000042000F01000001C042005C05
00000004000000010000000042007901000001A84200570500000004000000020000000042009101000
0019042000801000000030042000A07000000174372797074 6F6772617068696320416C676F72697468
```

```
42007801000002584200770100000088420069010000002042006A02000000040000000100000000042
006B020000000400000001000000000042000C010000004842002301000000404200240500000000040000
```

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

	Tag: 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: ccab716f-ce64-41f5-b42e-36ba4a894262 42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042 006B02000000040000000100000000420092090000000800000004F9A556B42000D02000000040000 0001000000000042000F010000006842005C0500000004000000010000000042007F0500000004000000 000000000042007C010000004042005705000000040000000200000000420094070000002463636162 373136662D636536342D343166352D623432652D33366261346138393432363200000000
1	Client A Get Attributes, Get In (header): credential={ credentialType='1', credentialValue={ username="Fred", password="password1" } } In: attributeName='Operation Policy Name' In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Authentication (0x42000C), Type: Structure (0x01), Data: Tag: Credential (0x420023), Type: Structure (0x01), Data: Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password) Tag: Credential Value (0x420025), Type: Structure (0x01), Data: Tag: Username (0x420099), Type: Text String (0x07), Data: Fred

```
        Tag: Password (0x4200A1), Type: Text String (0x07), Data: password1

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
55D88770E2556DAB

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ccab716f-
ce64-41f5-b42e-36ba4a894262

      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: Byte String (0x08), Data:
EB864EE01F1F98CD

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ccab716f-
ce64-41f5-b42e-36ba4a894262
```

```
42007801000001704200770100000088420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000C010000004842002301000000404200240500000004000
0000100000000420025010000002842009907000000044672656400000000004200A10700000009706173
73776F726431000000000000000042000D0200000004000000020000000042000F010000007842005C05
000000040000000B000000004200930800000000855D88770E2556DAB4200790100000050420094070000
0002463636162373136662D636536342D343166352D623432652D333662613461383934323632000000
000042000A070000000154F7065726174696F6E20506F6C696379204E616D650000000042000F01000000
5842005C0500000004000000000A0000000042009308000000008EB864EE01F1F98CD4200790100000030
42009407000000024636361623731366 62D636536342D343166352D623432652D333662613461383934
3236320000000
```

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:
```

```
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B
(Fri Apr 27 10:14:35 CEST 2012)

    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: Byte String (0x08), Data:
55D88770E2556DAB

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ccab716f-
ce64-41f5-b42e-36ba4a894262

      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: Byte String (0x08), Data:
EB864EE01F1F98CD

    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: ccab716f-
ce64-41f5-b42e-36ba4a894262

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
30E55F4B230B34CE8AFC476C66F8351B

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

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



42007B01000001D842007A0100000048420069010000002042006A0200000004000000010000000042
```

	006B020000000040000000100000000420092090000000080000000004F9A556B42000D0200000000400000 0002000000000042000F01000000A042005C0500000000400000000B00000000420093080000000855D887 70E2556DAB42007F050000000040000000000000000042007C0100000068420094070000002463636162 373136662D636536342D343166352D623432652D333662613461383934323632000000004200080100 00003042000A07000000154F7065726174696F6E20506F6C696379204E616D650000042000B070000 000764656661756C740042000F01000000D842005C0500000000400000000A000000004200930800000 08EB864EE01F1F98CD42007F050000000040000000000000000042007C01000000A04200570500000004 0000000200000000420094070000002463636162373136662D636536342D343166352D623432652D33 366261346138393432363200000000042008F01000000584200400100000050420042050000000040000 0001000000004200450100000018420043080000001030E55F4B230B34CE8AFC476C66F8351B420028 050000000400000003000000042002A0200000000400000080000000000

2	Client B
	Get (symmetric key), Get Attribute List
	In (header): credential={ credentialType=’1’, credentialValue={ username=”Barney”, password=”secret2” } }, BatchOrderOption=’true’, BatchErrorContinuationOption=’Continue’
	In: uuidKey
	In: uuidKey
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
	    Tag: Authentication (0x42000C), Type: Structure (0x01), Data:
	      Tag: Credential (0x420023), Type: Structure (0x01), Data:
	        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000001 (Username and Password)
	        Tag: Credential Value (0x420025), Type: Structure (0x01), Data:
	          Tag: Username (0x420099), Type: Text String (0x07), Data: Barney
	          Tag: Password (0x4200A1), Type: Text String (0x07), Data: secret2
	    Tag: Batch Error Continuation Option (0x42000E), Type: Enumeration (0x05), Data: 0x00000001 (Continue)
	    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: 0x0000000A (Get)

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
4F0E6D3DBA3D0495

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ccab716f-
ce64-41f5-b42e-36ba4a894262

  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: Byte String (0x08), Data: 
9B937E7CD50B233B

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ccab716f-
ce64-41f5-b42e-36ba4a894262
```

```
42007801000001684200770100000000A04200690100000020420006A020000000400000001000000042
006B02000000040000000100000000042000C01000000404200230100000038420024050000000040000
0001000000004200250100000020420099070000000064261726E657900004200A1070000000007736563
72657432004200 0E050000000400000001000000004200100600000008000000000000000142000D02
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B 
(Fri Apr 27 10:14:35 CEST 2012)

    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: Byte String (0x08), Data: 4F0E6D3DBA3D0495 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: Byte String (0x08), Data: 9B937E7CD50B233B 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 42007B010000011042007A0100000048420069010000002042006A0200000004000000010000000042 006B02000000040000000100000000420092090000000800000004F9A556B42000D020000000400000 0002000000000042000F010000005842005C0500000004000000A000000004200930800000084F0E6D 3DBA3D049542007F0500000004000000010000000042007E0500000004000000C000000042007D07 0000000D416363657373206465 6E69656400000042000F010000005842005C0500000004000000C00 000000420093080000000089B937E7CD50B233B42007F0500000004000000010000000042007E050000 0004000000C000000042007D070000000D4163636573732064656E696564000000
3	Destroy In (header): credential={ credentialType='1', credentialValue={ username="Fred", password="password1" } } In: uuidKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Authentication (0x42000C), Type: Structure (0x01), Data:

```
      Tag: Credential (0x420023), Type: Structure (0x01), Data:

        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 
0x00000001 (Username and Password)

        Tag: Credential Value (0x420025), Type: Structure (0x01), Data:

          Tag: Username (0x420099), Type: Text String (0x07), Data: Fred

          Tag: Password (0x4200A1), Type: Text String (0x07), Data: password1

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

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

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ccab716f-
ce64-41f5-b42e-36ba4a894262
```

```
42007801000000E04200770100000088420069010000002042006A0200000004000000010000000042
006B020000000400000001000000000042000C0100000048420023010000004042002405000000040000
0001000000004200250100000028420099070000000446726564000000004200A10700000009706173
73776F72643100000000000000042000D0200000004000000010000000042000F010000004842005C05
00000004000000140000000042007901000000304200940700000024636361623731366662D63653634
2D343166352D623432652D33366261346138393432363200000000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B 
(Fri Apr 27 10:14:35 CEST 2012)

    Tag: 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: ccab716f-
ce64-41f5-b42e-36ba4a894262
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000000004F9A556B42000D020000000400000
00010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000
000000000042007C0100000030420094070000002463636162373136662D636536342D343166352D62
3432652D33366261346138393432363200000000
```

4

Get Attributes

In (header): credential={ credentialType='1', credentialValue={ username="Fred", password="password1" } }

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

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Authentication (0x42000C), Type: Structure (0x01), Data:

      Tag: Credential (0x420023), Type: Structure (0x01), Data:

        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data:
0x00000001 (Username and Password)

        Tag: Credential Value (0x420025), Type: Structure (0x01), Data:

          Tag: Username (0x420099), Type: Text String (0x07), Data: Fred

          Tag: Password (0x4200A1), Type: Text String (0x07), Data: password1

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

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

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: ccab716f-
ce64-41f5-b42e-36ba4a894262

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

```
42007801000000F84200770100000088420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000C0100000048420023010000004042002405000000040000
0001000000004200250100000028420099070000000446726564000000004200A107000000009706173
73776F7264310000000000000042000D0200000004000000010000000042000F01000000604200 5C05
00000004000000B00000000420079010000004842009407000000246363616237313666 2D63653634
2D343166352D623432652D33366261346138393432363200000000042000A070000000C44657374726F
7920446174650000000
```

Out: uuidKey, attributes={ DestroyDate=’ 0x000000004B9F8B4D’ }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B
(Fri Apr 27 10:14:35 CEST 2012)

    Tag: 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: ccab716f-
ce64-41f5-b42e-36ba4a894262

      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:
0x000000004F9A556B (Fri Apr 27 10:14:35 CEST 2012)
```

```
42007B01000000E042007A0100000048420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042009209000000080000000004F9A556B42000D0200000004000 0
00010000000042000F010000008842005C05000000040000000B00000000042007F0500000004000000
0000000000042007C010000006042009407000000246363616237313666 2D636536342D343166352D62
3432652D3336626134613839343236320000000004200080100000028 42000A070000000C4465737472
6F7920446174650000000042000B090000000800000000 4F9A556B
```

11.2 Test Case: Device Credential, Operation Policy, Destroy Date

Pass a Credential object of type Device Credential in the message header in all requests for identification purposes (how the Credential object is used is defined in [KMIP-Spec]

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof]). Create a symmetric key and set the Operation Policy Name attribute to “default”. Using another Credential, attempt to perform a Get operation batched with a Get Attribute List on the created symmetric key – according to the Default Operation Policy, both these request SHALL fail, and with the Batch Error Continuation Option set to “Continue”, the client SHALL also receive both response payloads. Using the initially used Credential, destroy the object and get the Destroy Date attribute.

The message exchanges in this test case are based on a certain server policy (e.g. handling of Credentials) that in some aspects differs from the policy assumed in earlier test cases (e.g. in this test case, the Destroy Date is retained). The message exchanges shown in this test case assume that both Credentials used in this example are for valid users of the server. As mentioned in Section 1 , the message exchanges shown in this document are not the only correct alternatives.

Time	Request/Response messages

0	Client A
	Create (symmetric key)
	In (header): credential={ credentialType=’2’, credentialValue={ deviceSerialNumber='serNum123456', password='secret', deviceIdentifier='devID2233', networkIdentifier='netID9000', machineIdentifier='machineID1', mediaIdentifier='mediaID313' } }
	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: 
0x00000001 (1)

    Tag: Authentication (0x42000C), Type: Structure (0x01), Data: 

      Tag: Credential (0x420023), Type: Structure (0x01), Data: 

        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 
0x00000002 (Device)

        Tag: Credential Value (0x420025), Type: Structure (0x01), Data: 

          Tag: Device Serial Number (0x4200B0), Type: Text String (0x07), Data: 
serNum123456

          Tag: Password (0x4200A1), Type: Text String (0x07), Data: secret

          Tag: Device Identifier (0x4200A2), Type: Text String (0x07), Data: 
devID2233

          Tag: Network Identifier (0x4200AB), Type: Text String (0x07), Data: 
netID9000

          Tag: Machine Identifier (0x4200A9), Type: Text String (0x07), Data: 
machineID1

          Tag: Media Identifier (0x4200AA), Type: Text String (0x07), Data: 
mediaID313

    Tag: 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)
```

```
42007801000002B042007701000000E8420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000C01000000A842002301000000A042002405000000040000
00020000000042002501000000884200B0070000000C7365724E756D31323334353600000004200A1
07000000067365637265740000004200A207000000096465764944323233330000000000000004200AB07
000000096E6574494439303030000000000000004200A9070000000A6D616368696E65494431000000
0000004200AA070000000A6D6564696149443331330000000000000042000D0200000004000000010000
000042000F01000001B842005C0500000004000000010000000042007901000001A042005705000000
04000000020000000042009101000001884200080100000030420000A070000000174372797074F6772
617068696320416C676F726974686D0042000B05000000040000000300000000420008010000003042
000A070000001443727970746F6772617068696320C656E677468000000042000B02000000040000
0080000000004200080100000030420000A0700000018437279707468F677261706869632055736167 65
204D61736B42000B020000000400000000C00000000420008010000004042000A07000000044E616D65
0000000042000B010000002842005507000000009506F6C6963794B6579000000000000000004200540500
00000400000001000000004200080100000030420000A07000000154F7065726174696F6E20506F6C69
6379204E616D650000000042000B07000000076465666175C7400420008010000005842000A07000000
184372797074F677261706869632050617261D657465727342000B010000003042001105000000004
0000000100000000042005F050000000400000003000000004200380500000000400000000400000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B 
(Fri Apr 27 10:14:35 CEST 2012)
    Tag: 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: b272543a-
6558-4e47-9221-3d291c93e9b5
```

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A556B42000D020000000400000
00010000000042000F010000006842005C0500000004000000010000000042007F0500000004000000
0000000000042007C010000004042005705000000040000000200000000420094070000002462323732
353433612D363535382D346534372D393232312D336432393163393365396235000000000
```

1

Client A

Get Attributes, Get

In (header): credential={ credentialType='2', credentialValue={ deviceSerialNumber='serNum123456', password='secret', deviceIdentifier='devID2233', networkIdentifier='netID9000', machineIdentifier='machineID1', mediaIdentifier='mediaID313' } }

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: 
0x00000001 (1)

    Tag: Authentication (0x42000C), Type: Structure (0x01), Data: 

      Tag: Credential (0x420023), Type: Structure (0x01), Data: 

        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 
0x00000002 (Device)

        Tag: Credential Value (0x420025), Type: Structure (0x01), Data: 

          Tag: Device Serial Number (0x4200B0), Type: Text String (0x07), Data: 
serNum123456

          Tag: Password (0x4200A1), Type: Text String (0x07), Data: secret

          Tag: Device Identifier (0x4200A2), Type: Text String (0x07), Data: 
devID2233

          Tag: Network Identifier (0x4200AB), Type: Text String (0x07), Data: 
netID9000

          Tag: Machine Identifier (0x4200A9), Type: Text String (0x07), Data: 
machineID1

          Tag: Media Identifier (0x4200AA), Type: Text String (0x07), Data: 
mediaID313

    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: Byte String (0x08), Data: 
E705E27DC0BA7789

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b272543a-
6558-4e47-9221-3d291c93e9b5

      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: Byte String (0x08), Data: 
50A7F741A1119826

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b272543a-
6558-4e47-9221-3d291c93e9b5



42007801000001D042007701000000E842006901000000204200 6A02000000040000000100000000 42
006B02000000040000000100000000 42000C01000000A842002301000000A04200240500000004 0000
000200000000420025010000008842 00B0070000000C7365724E756D3132333435360000000 04200A1
0700000006736563726574000042 00A20700000009646576494432323333000000000000004200AB07
000000096E6574494439303030000000000000004200A9070000000A6D616368696E65494431000000
0000004200AA070000000A6D656469614944333133000000000000000042000D0200000004000000020000
```

000042000F010000007842005C0500000004000000000B00000000420093080000000 8E705E27DC0BA77

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B
(Fri Apr 27 10:14:35 CEST 2012)

    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: Byte String (0x08), Data:
E705E27DC0BA7789

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b272543a-
6558-4e47-9221-3d291c93e9b5

      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: Byte String (0x08), Data:
50A7F741A1119826

    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: b272543a-
6558-4e47-9221-3d291c93e9b5

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
ACFEAFFDBDD17D0E63624A22083EE4B6

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

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

```
42007B01000001D842007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A556B42000D020000000400000
0002000000000042000F01000000A042005C0500000004000000000B00000000420093080000008E705E2
7DC0BA778942007F05000000040000000000000000042007C010000006842009407000000246232373 2
353433612D363535382D346534372D393232312D336432393163393365396235000000004200080100
00003042000A07000000154F7065726174696F6E20506F6C696379204E616D650000000042000B070000
000764656661756C740042000F01000000D842005C0500000004000000000A00000000420093080000000
0850A7F741A111982642007F05000000040000000000000000042007C01000000A04200570500000004
000000020000000042009407000000246232373235343361 2D363535382D346534372D393232312D33
643239316339336539623500000000042008F01000000584200400100000050420042050000000400000
00010000000042004501000000184200430800000010ACFEAFFDBDD17D0E63624A22083EE4B6420028
05000000040000000300000000042002A02000000040000008000000000
```

2

Client B

Get (symmetric key), Get Attribute List

In (header): credential={ credentialType=’2’, credentialValue={ deviceSerialNumber='serNum101010', password='passwd', deviceIdentifier='devID4444', networkIdentifier='netID9', machineIdentifier='machineID1111', mediaIdentifier='mediaID0000' } }, 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: 
0x00000001 (1)

    Tag: Authentication (0x42000C), Type: Structure (0x01), Data:

      Tag: Credential (0x420023), Type: Structure (0x01), Data:

        Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 
0x00000002 (Device)

        Tag: Credential Value (0x420025), Type: Structure (0x01), Data:

          Tag: Device Serial Number (0x4200B0), Type: Text String (0x07), Data: 
serNum101010

          Tag: Password (0x4200A1), Type: Text String (0x07), Data: passwd

          Tag: Device Identifier (0x4200A2), Type: Text String (0x07), Data: 
devID4444

          Tag: Network Identifier (0x4200AB), Type: Text String (0x07), Data: 
netID9

          Tag: Machine Identifier (0x4200A9), Type: Text String (0x07), Data: 
machineID1111

          Tag: Media Identifier (0x4200AA), Type: Text String (0x07), Data: 
mediaID0000

    Tag: Batch Error Continuation Option (0x42000E), Type: Enumeration (0x05), 
Data: 0x00000001 (Continue)

    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: 0x0000000A (Get)

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
1154049D742C498E

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b272543a-
6558-4e47-9221-3d291c93e9b5

  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: Byte String (0x08), Data: 
8AE55C6E91D97B05

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: b272543a-
```

```
6558-4e47-9221-3d291c93e9b5
```

```
42007801000001C84200770100000100420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000C01000000A042002301000000984200240500000004000
00020000000042002501000000804200B0070000000C7365724E756D3130313031300000000004200A1
07000000067061737377640000 4200A207000000096465764944343434340000000000000004200AB07
000000066E657449443900004200A9070000000D6D616368696E6549443131313100000004200AA0700
00000B6D656469614944303030300000000000042000E050000000400000001000000004200100600000
0080000000000000000142000D020000000400000002000000042000F01000000584200 5C05000000
040000000A000000004200930800000008115404 9D742C498E420079010000003042009407000000024
62323732353433612D363535382D346534372D393232312D336432393163393365396235000000000042
000F01000000584200 5C050000000400000000C000000004200930800000088AE55C6E91D97B054200
790100000030420094070000002462323732353433612D363535382D346534372D393232312D336432
3931633933653962350000000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B
(Fri Apr 27 10:14:35 CEST 2012)
    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: Byte String (0x08), Data:
1154049D742C498E
    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: Byte String (0x08), Data:
```

	8AE55C6E91D97B05 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 42007B010000011042007A0100000048420069010000002042006A02000000040000000100000000420 06B0200000004000000010000000042009209000000080000000004F9A556B42000D02000000040000 00020000000042000F010000005842005C0500000004000000A00000000420093080000000081154049 D742C498E42007F0500000004000000010000000042007E05000000040000000C0000000042007D07 0000000D4163636573732064656E6965640000000042000F010000005842005C05000000040000000C00 000000420093080000000088AE55C6E91D97B0542007F05000000040000000100000000042007E050000 00040000000C0000000042007D070000000D4163636573732064656E696564000000
3	Client A Destroy In (header): credential={ credentialType=’2’, credentialValue={ deviceSerialNumber='serNum123456', password='secret', deviceIdentifier='devID2233', networkIdentifier='netID9000', machineIdentifier='machineID1', mediaIdentifier='mediaID313' } } 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: 0x00000001 (1) Tag: Authentication (0x42000C), Type: Structure (0x01), Data: Tag: Credential (0x420023), Type: Structure (0x01), Data: Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000002 (Device) Tag: Credential Value (0x420025), Type: Structure (0x01), Data: Tag: Device Serial Number (0x4200B0), Type: Text String (0x07), Data: serNum123456 Tag: Password (0x4200A1), Type: Text String (0x07), Data: secret Tag: Device Identifier (0x4200A2), Type: Text String (0x07), Data:

```
devID2233

          Tag: Network Identifier (0x4200AB), Type: Text String (0x07), Data: 
netID9000

          Tag: Machine Identifier (0x4200A9), Type: Text String (0x07), Data: 
machineID1

          Tag: Media Identifier (0x4200AA), Type: Text String (0x07), Data: 
mediaID313

    Tag: 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: b272543a-
6558-4e47-9221-3d291c93e9b5
```

```
420078010000014042007701000000E8420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000C01000000A842002301000000A042002405000000040000
00020000000042002501000000884200B0070000000C7365724E756D313233343536000000004200A1
070000000673656372657400004200A20700000009646576494432323333000000000000004200AB07
000000096E6574494439303030000000000000004200A9070000000A6D616368696E65494431000000
0000004200AA070000000A6D65646961494433313300000000000042000D0200000004000000010000
000042000F010000004842005C050000000400000014000000004200790100000030420094070000000
246232373235343361 2D363535382D346534372D393232312D33643239316339336539623500000000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B 
(Fri Apr 27 10:14:35 CEST 2012)

    Tag: 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: b272543a-6558-4e47-9221-3d291c93e9b5 42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420 06B02000000040000000100000000420092090000000800000004F9A556B42000D02000000040000 00010000000042000F010000005842005C0500000004000000140000000042007F05000000040000000 0000000000042007C010000003042009407000000246232373235343361 2D363535382D346534372D39 3232312D336432393163393365396235 00000000
4	Client A Get Attributes In (header): credential={ credentialType=’2’, credentialValue={ deviceSerialNumber='serNum123456', password='secret', deviceIdentifier='devID2233', networkIdentifier='netID9000', machineIdentifier='machineID1', mediaIdentifier='mediaID313' } } 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: 0x00000001 (1) Tag: Authentication (0x42000C), Type: Structure (0x01), Data: Tag: Credential (0x420023), Type: Structure (0x01), Data: Tag: Credential Type (0x420024), Type: Enumeration (0x05), Data: 0x00000002 (Device) Tag: Credential Value (0x420025), Type: Structure (0x01), Data: Tag: Device Serial Number (0x4200B0), Type: Text String (0x07), Data: serNum123456 Tag: Password (0x4200A1), Type: Text String (0x07), Data: secret Tag: Device Identifier (0x4200A2), Type: Text String (0x07), Data: devID2233 Tag: Network Identifier (0x4200AB), Type: Text String (0x07), Data: netID9000

```
          Tag: Machine Identifier (0x4200A9), Type: Text String (0x07), Data: 
machineID1

          Tag: Media Identifier (0x4200AA), Type: Text String (0x07), Data: 
mediaID313

    Tag: 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: b272543a-
6558-4e47-9221-3d291c93e9b5

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

```
42007801000001584200770100000000E84200690100000002042006A02000000040000000100000000042
006B02000000040000000100000000042000C01000000A842002301000000A042002405000000040000
000200000000042002501000000884200B0070000000C7365724E756D31323334353600000004200A1
07000000067365637265740000004200A207000000096465764944323233330000000000000004200AB07
000000096E65744944393030300000000000000004200A9070000000A6D616368696E65494431000000
0000004200AA070000000A6D6564696149443331330000000000000042000D02000000040000000010000
000042000F01000000060420005C05000000040000000B0000000042007901000000484200940700000000
2462323732353433612D363535382D346534372D393232312D3364323931633933653962350000000000
42000A070000000C44657374726F79204461746500000000
```

Out: uuidKey, attributes={ DestroyDate='0x000000004E4D0F63' }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B 
(Fri Apr 27 10:14:35 CEST 2012)

    Tag: 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: b272543a-
6558-4e47-9221-3d291c93e9b5

      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:
0x000000004F9A556B (Fri Apr 27 10:14:35 CEST 2012)
```

```
42007B01000000E042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A556B42000D020000000400000
00010000000042000F010000008842005C050000000400000000B000000042007F0500000004000000
000000000042007C0100000060420094070000002462323732353433612D363535382D346534372D39
3232312D336432393163393365396235000000004200080100000002842000A070000000C4465737472
6F792044617465000000000042000B090000000800000004F9A556B
```

12 Query, Maximum Response Size

This section contains test cases that exercise the Query operation and the Maximum Response Size header field.

12.1 Test Case: Query, Maximum Response Size

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 messages

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: 0x00000001 (1)
	    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 (Query Operations)
	      Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000002 (Query Objects)
	42007801000000904200770100000048420069010000002042006A02000000040000000100000000042
	006B020000000400000001000000004200500200000004000001000000000042000D0200000000040000

	00010000000042000F010000003842005C050000000400000018000000004200790100000020420074 0500000004000000010000000420074050000000400000002000000000 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: 0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B (Fri Apr 27 10:14:35 CEST 2012) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: 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: 648, Maximum Response Size indicated in request: 256 42007B01000000C842007A0100000048420069010000002042006A02000000040000000100000000042 006B02000000040000000100000000420092090000000800000004F9A556B42000D0200000004000 00001000000000042000F010000007042007F05000000040000000100000000042007E050000000400000 020000000042007D070000004352657370 6F6E73652073697A653A203634382C204D6178696D756D20 526573706F6E73652053697A6520696E64696361746564 20696E2072657175657374 3A2032353 60000 000000
1	Query (operations, objects) In (header): maximumResponseSize='2048' In: queryFunctions={ '00000001', '00000002', '00000003' } Tag: Request Message (0x420078), Type: Structure (0x01), Data:

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    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 
(Query Operations)

      Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000002 
(Query Objects)

      Tag: Query Function (0x420074), Type: Enumeration (0x05), Data: 0x00000003 
(Query Server Information)
```

```
42007801000000A04200770100000048420069010000002042006A02000000040000000100000000 42
006B020000000400000001000000004200500200000004000008000000000042000D020000000400000
00010000000042000F010000004842005C050000000400000018000000004200790100000030420074
05000000040000000100000000420074050000000400000002000000004200740500000004000000 03
00000000
```

Out: operations, objects, serverInformation

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B 
(Fri Apr 27 10:14:35 CEST 2012)

    Tag: 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: 0x00000006
(Certify)
      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000007 (Re-
certify)
      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: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001D (Re-
key Key Pair)

      Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001E 
(Discover Versions)

      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)

      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000007 
(Secret Data)

      Tag: Vendor Identification (0x42009D), Type: Text String (0x07), Data: IBM 
test server, not-TKLM 2.0.1.1 KMIP 2.0.0.1

      Tag: Server Information (0x420088), Type: Structure (0x01), Data: null
```

```
42007B01000002C042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000000400000001000000004200920900000008000000004F9A556B42000D02000000040000
0001000000000042000F010000026842005C0500000004000000180000000042007F0500000004000000
0000000000042007C010000024042005C0500000004000000010000000042005C050000000400000002
0000000042005C0500000004000000030000000042005C0500000004000000040000000042005C0500
0000040000000600000000042005C0500000004000000070000000042005C05000000040000000080000
000042005C0500000004000000090000000042005C050000000400000000A000000042005C05000000
040000000B000000042005C0500000004000000C000000042005C050000000400000000D00000000
42005C0500000004000000E0000000042005C050000000040000000F000000042005C050000000400
00001000000000042005C0500000004000000110000000042005C05000000040000001200000000004200
5C0500000004000000130000000042005C05000000040000001400000000042005C050000000004000000
1500000000042005C05000000040000001600000000042005C05000000040000001800000000042005C05
00000004000000190000000042005C050000000040000001A000000042005C050000000040000001D00
0000042005C05000000004000001E000000004200570500000004000000010000000042005705000
0004000000002000000004200570500000004000000030000000042005705000000040000000004000000
00420057050000000400000006000000004200570500000004000000070000000042009D070000002E
49424D2074657374207365727665722C206E6F742D544B4C4D20322E302E312E31204B4D495020322E
302E302E3100004200880100000000
```

12.2 Test Case: Query Vendor Extensions

Query the server for a list and map of vendor extension tags it recognizes.

Time	Request/Response messages
0	Query (extension list) In: queryFunctions={ '00000005' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: 0x00000005 (Query Extension List) 42007801000000704200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000010000000042000D0200000004000000010000000042000F010000002842005C05000000040000001800000000420079010000001042007405000000040000000500000000 Out: extension list Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B (Fri Apr 27 10:14:35 CEST 2012)

```
    Tag: 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: Extension Information (0x4200A4), Type: Structure (0x01), Data:

        Tag: Extension Name (0x4200A5), Type: Text String (0x07), Data: ACME
LOCATION

      Tag: Extension Information (0x4200A4), Type: Structure (0x01), Data:

        Tag: Extension Name (0x4200A5), Type: Text String (0x07), Data: ACME ZIP
CODE


42007B01000000C042007A0100000048420069010000002042006A02000000040000000100000000042
006B020000000400000001000000004200920900000008000000004F9A556B42000D020000000400000
00010000000042000F01000000684200 5C050000000400000018000000042007F050000000040000000
00000000042007C010000004042 00A4010000001842 00A5070000000D41434D45204C4F434154494F
4E0000004200A40100000018420 0A5070000000D41434D45205A495020434F4445000000
```

1

Query (extension map)

In: queryFunctions={ '00000006' }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: 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: 0x00000006
(Query Extension Map)


42007801000000704200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000284200
```

```
5C050000000400000018000000004200790100000010420074050000000400000006000000000
```

Out: extension map

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556B 
(Fri Apr 27 10:14:35 CEST 2012)
    Tag: 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: Extension Information (0x4200A4), Type: Structure (0x01), Data:
        Tag: Extension Name (0x4200A5), Type: Text String (0x07), Data: ACME 
LOCATION
        Tag: Extension Tag (0x4200A6), Type: Integer (0x02), Data: 0x0054AA01 
(5548545)
        Tag: Extension Type (0x4200A7), Type: Integer (0x02), Data: 0x00000007 (7)
      Tag: Extension Information (0x4200A4), Type: Structure (0x01), Data:
        Tag: Extension Name (0x4200A5), Type: Text String (0x07), Data: ACME ZIP 
CODE
        Tag: Extension Tag (0x4200A6), Type: Integer (0x02), Data: 0x0054AA02 
(5548546)
        Tag: Extension Type (0x4200A7), Type: Integer (0x02), Data: 0x00000002 (2)
```

```
42007B01000001004200 7A0100000048420069010000002042006A020000000400000001000000042
```

13 Asymmetric Keys and Certificates

The test cases in this section deal with asymmetric keys and certificates using the operations, objects, attributes and key formats specified in the asymmetric key profiles in [KMIP-Spec]

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof].

13.1 Test Case: Register an Asymmetric Key Pair in PKCS#1 Format

Register a private key in the PKCS#1 key format, then register the corresponding public key, also in PKCS#1 format, with the Link attribute pointing to the previously registered private key. Thereafter add the Link attribute to the private key, and perform Locate-commands to find the public and private keys using the Link attribute. Get both the private and public keys in PKCS#1 key format, before finally destroying both the private and the public key.

This test case is aimed at exercising the functionality defined in the Basic Asymmetric Key Profile [KMIP-Spec]

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof].

Time	Request/Response messages

0	Register (Private Key)
	In: objectType='00000004', attributes={ CryptographicUsageMask='00000001' }, privateKey
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
	    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)

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

    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003
(Register)

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

      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000004
(Private Key)

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

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

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

          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000001
(Sign)

      Tag: Private Key (0x420064), Type: Structure (0x01), Data:

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

          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data:
0x00000003 (PKCS#1)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
308204A50201000282010100AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E44
0AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7
EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A411
00F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC829
5353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA8
09E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374
FE30E54951662A6EDA29C6FC411335D5DC7426B0F6050203010001028201003B12455D53C1816516C5
18493F6398AAFA72B17DFA894DB888A7D48C0A47F62579A4E644F86DA711FEC850CDD9DBBD17F69A44
3D2EC1DD60D3C618FA74CDE5FDAFABD6BAA26EB0A3ADB4DEF6480FB1218CD3B083E252E885B6F0729F
98B2144D2B72293E1B11D73393BC41F75B15EE3D7569B4995ED1A14425DA4319B7B26B0E8FEF17C375
42AE5C6D5849F87209567F3925A47B016D564859717BC57FCB4522D0AA49CE816E5BE7B3088193236E
C9EFFF140858045B73C5D79BAF38F7C67F04C5DCF0E3806AD982D1259058C3473E847179A878F2C6B3
BD968FB99EA46E9185892F3676E78965C2AED4877BA3917DF07C5E927474F19E764BA61DC38D63BF29
02818100D5C69C8C3CDC2464744A793713DAFB9F1DBC799FF96423FECD3CBA794286BCE920F4B5C183
F99EE9028DB6212C6277C4C8297FCFBCE7F7C24CA4C51FC7182FB8F4019FB1D5659674C5CBE6D5FA99
2051341760CD00735729A070A9E54D342BEBA8EF47EE82D3A01B04CEC4A00D4DDB41E35116FC221E85
4B43A696C0E6419B1B02818100CD5EA7702789064B673540CBFF09356AD80BC3D592812EBA47610B9F
AC6AECEFE22ACAE438459CDA74E59653D88C04189D34399BF5B14B920E34EF38A7D09FE69593396E8F
E735E6F0A6AE4990401041D8A406B6FD86A1161E45F95A3EAA5C1012E6662E44F15F335AC971E1766B
2BB9C985109974141B44D37E1E319820A55F02818100B2871237BF9FAD38C3316AB7877A6A868063E5
42A7186D431E8D27C19AC0414584033942E9FF6E2973BB7B2D8B0E94AD1EE82158108FBC8664517A5A
467FB963014BD5DCC2B4FB087C23039D11920DBE22FD9F16B4D89E23225CD455ADBAF32EF43F185864
A36D630309D6853F7714B39AAE1EBEE3938F87C2707E178C739F9F028181009690BED14B2AFAA26D98
6D592231EE27D71D49065BD2BA1F78157E20229881FD9D23227D0F8479EAEFA922FD75D5B16B1A561F
A6680B040CA0BDCE650B23B917A4B1BB7983A74FAD70E1C305CBEC2BFF1A85A726A1D90260E4F1084F
518234DCD3FE770B9520215BD543BB6A4117718754676A34171666A79F26E79C149C5AA102818100A0
C985A0A0A791A659F99731134C44F37B2E520A2CEA35800AD27241ED360DFDE6E8CA614F12047FD08B
76AC4D13C056A0699E2F98A1CAC91011294D71208F4ABAB33BA87AA0517F415BACA88D6BAC006088FA
601D349417E1F0C9B23AFFA4D496618DBC024986ED690BBB7B025768FF9DF8AC15416F489F8129C323
41A8B44F

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000800 (2048)
```

```
42007801000005B04200770100000038420069010000002042006A02000000040000000100000000042
006B02000000004000000010000000042000D02000000004000000010000000042000F01000005684200
5C050000000040000000300000000420079010000055042005705000000004000000040000000420091
01000000384200080100000030420000A07000000184372797074667726170686963205573616765520
4D61736B42000B020000000040000000100000000420064010000004F842004001000004F04200420500
000004000000003000000004200450100004B842004308000004A9308204A50201000282010100AB7F
161C0042496CCD6C6D4DADB91997343535777600 3ACF54B7AF1E440AFB80B64A8755F8002CFEBA6B18
4540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7EC114F3B176B7957C422E7D03FC6
267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA214900DF8B65089F98135B
1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C795328ABF70E1B42E7BB8B7
F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1B7AE64C54130FBC21D80E9
C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E54951662A6EDA29C6FC4113
35D5DC7426B0F605020301000102820100 3B12455D53C1816516C518493F6398AAFA72B17DFA894DB8
88A7D48C0A47F62579A4E644F86DA711FEC850CDD9DBBD17F69A443D2EC1DD60D3C618FA74CDE5FDAF
ABD6BAA26EB0A3ADB4DEF6480FB1218CD3B083E252E885B6F0729F98B2144D2B72293E1B11D73393BC
41F75B15EE3D7569B4995ED1A14425DA4319B7B26B0E8FEF17C37542AE5C6D5849F87209567F3925A4
7B016D564859717BC57FCB4522D0AA49CE816E5BE7B3088193236EC9EFFF140858045B73C5D79BAF38
F7C67F04C5DCF0E3806AD982D1259058C3473E847179A878F2C6B3BD968FB99EA46E9185892F3676E7
8965C2AED4877BA3917DF07C5E927474F19E764BA61DC38D63BF2902818100D5C69C8C3CDC2464744A
793713DAFB9F1DBC799FF96423FECD3CBA794286BCE920F4B5C183F99EE9028DB6212C6277C4C8297F
CFBCE7F7C24CA4C51FC7182FB8F4019FB1D5659674C5CBE6D5FA992051341760CD00735729A070A9E5
4D342BEBA8EF47EE82D3A01B04CEC4A00D4DDB41E35116FC221E854B43A696C0E6419B1B02818100CD
5EA7702789064B673540CBFF09356AD80BC3D592812EBA47610B9FAC6AECEFE22ACAE438459CDA74E5
9653D88C04189D34399BF5B14B920E34EF38A7D09FE69593396E8FE735E6F0A6AE4990401041D8A406
B6FD86A1161E45F95A3EAA5C1012E6662E44F15F335AC971E1766B2BB9C985109974141B44D37E1E31
9820A55F02818100B2871237BF9FAD38C3316AB7877A6A868063E542A7186D431E8D27C19AC0414584
033942E9FF6E2973BB7B2D8B0E94AD1EE82158108FBC8664517A5A467FB963014BD5DCC2B4FB087C23
039D11920DBE22FD9F16B4D89E23225CD455ADBAF32EF43F185864A36D630309D6853F7714B39AAE1E
BEE3938F87C2707E178C739F9F028181009690BED14B2AFAA26D986D592231EE27D71D49065BD2BA1F
78157E20229881FD9D23227D0F8479EAEFA922FD75D5B16B1A561FA6680B040CA0BDCE650B23B917A4
B1BB7983A74FAD70E1C305CBEC2BFF1A85A726A1D90260E4F1084F518234DCD3FE770B9520215BD543
BB6A4117718754676A34171666A79F26E79C149C5AA102818100A0C985A0A0A791A659F99731134C44
F37B2E520A2CEA35800AD27241ED360DFDE6E8CA614F12047FD08B76AC4D13C056A0699E2F98A1CAC9
1011294D71208F4ABAB33BA87AA0517F415BACA88D6BAC006088FA601D349417E1F0C9B23AFFA4D496
618DBC024986ED690BBB7B025768FF9DF8AC15416F489F8129C32341A8B44F00000000000000420028
0500000004000000040000000042002A0200000000400008000000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556C
(Fri Apr 27 10:14:36 CEST 2012)
```

	Tag: 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: 7cf5209b-6ff6-4426-899e-22b067859372 42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042 006B02000000040000000100000000420092090000000800000004F9A556C42000D02000000040000 0001000000000042000F010000005842005C05000000040000000300000000042007F0500000004000000 000000000042007C0100000030420094070000002437636635323039622D366666362D343432362D38 3939652D32326230363738353933373200000000
1	Register (Public Key) In: objectType='00000003', attributes={ CryptographicUsageMask='00000002', Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } }, publicKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: 7cf5209b-6ff6-4426-899e-22b067859372

      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:
0x00000003 (PKCS#1)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
3082010A0282010100AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E440AFB80
B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7EC114F
3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA
214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C7
95328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1
B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E5
4951662A6EDA29C6FC411335D5DC7426B0F6050203010001

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000800 (2048)



42007801000002704200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000002284200
5C05000000040000000300000000420079010000021042005705000000040000000300000000420091
0100000098420008010000003042000A070000001843727970746F67726170686963205573616765204D61736B
```

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556C
(Fri Apr 27 10:14:36 CEST 2012)
    Tag: 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: 57492708-
09e8-4235-ab77-8eee6ed4647f
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A556C42000D020000000400000
00010000000042000F010000005842005C050000000400000003000000042007F05000000040000000
000000000042007C010000003042009407000000243537343932373082D303965382D343233352D61
6237372D386565653665643436343766000000000
```

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:
0x00000001 (1)
    Tag: 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: 7cf5209b-
6ff6-4426-899e-22b067859372

      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: 57492708-09e8-4235-ab77-8eee6ed4647f
```

```
42007801000000F04200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000A84200
5C05000000040000000D00000000420079010000009042009407000000243763663532303962 2D3666
66362D343432362D383939652D32326230363738353933373200000000420008010000005842000A07
000000044C696E6B0000000042000B01000000404 2004B05000000040000010200000000042004C0700
0000243537343932373038 2D303965382D343233352D616237372D38656565366564343634376600000
0000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556C
(Fri Apr 27 10:14:36 CEST 2012)

    Tag: 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: 7cf5209b-6ff6-4426-899e-22b067859372 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: 57492708-09e8-4235-ab77-8eee6ed4647f 42007B010000011042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000100000000420092090000000800000004F9A556C42000D0200000004000000010000000042000F01000000B842005C0500000004000000D000000000042007F0500000004000000000000000042007C010000009042009407000000243763663532303962 2D366666362D343432362D383939652D323262303637383539333732000000004200080100000058420000A07000000044C696E6B0000000042000B010000004042004B05000000040000010200000000042004C0700000024353734393237 30382D303965382D343233352D616237372D3865656536656434363437660000000
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: 0x00000001 (1) Tag: 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: 7cf5209b-6ff6-4426-899e-22b067859372
```

```
42007801000000F042007701000000384200690100000020042006A020000000400000001000000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000A84200
5C0500000004000000080000000042007901000000904200080100000028420000A070000000B4F626A
656374205479706500000000000042000B050000000400000003000000004200080100000058420000A07
000000044C696E6B0000000042000B01000000404200004B050000000400000103000000000042004C0700
000002437636635323039622D366666362D343432362D383939652D323262303637383539333732000
0000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556C
(Fri Apr 27 10:14:36 CEST 2012)
    Tag: 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: 57492708-
09e8-4235-ab77-8eee6ed4647f
```

```
42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000000042
006B020000000400000001000000004200920900000008000000004F9A556C42000D02000000040000
00010000000042000F010000005842005C05000000040000000800000000042007F0500000004000000
0000000000042007C01000000304200940700000024353734393237303382D303965382D343233352D61
```

```
6237372D38656565366564343634376600000000
```

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: 
0x00000001 (1)
    Tag: 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: 57492708-09e8-4235-ab77-8eee6ed4647f
```

```
42007801000000F04200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000A84200
5C05000000040000000800000000420079010000009042000801000000284200 0A070000000B4F626A
656374205479706500000000042000B05000000040000000400000000420008010000005842000A07
000000044C696E6B0000000042000B01000000404200 4B05000000040000010200000000042004C0700
00002435373439323730382D303965382D343233352D616237372D38656565366564343634376600000
0000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556C
(Fri Apr 27 10:14:36 CEST 2012)

    Tag: 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: 7cf5209b-
6ff6-4426-899e-22b067859372
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A556C42000D020000000400000
0001000000000042000F01000000584200 5C0500000004000000080000000042007F0500000004000000
000000000042007C01000000304200940700000024376366353230396 22D366666362D343432362D38
3939652D3232623036373835393337320000000 0
```

5

Get (private key)

In: uuidPrivateKey, keyFormatType='00000003'

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
```

```
    Tag: 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: 7cf5209b-6ff6-4426-899e-22b067859372
      Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000003 (PKCS#1)
```

```
42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000584200
5C05000000040000000A000000004200790100000040420094070000002437636635323039622D3666
66362D343432362D383939652D32326230363738353933373200000000420042050000000400000003
00000000
```

Out: objectType = ‘00000004’, uuidPrivateKey, privateKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556C (Fri Apr 27 10:14:36 CEST 2012)
    Tag: 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: 0x00000004 (Private Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 7cf5209b-6ff6-4426-899e-22b067859372
      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:
0x00000003 (PKCS#1)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
308204A502010002820101000AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E44
0AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7
EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A411
00F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC829
5353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA8
09E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374
FE30E54951662A6EDA29C6FC411335D5DC7426B0F6050203010001028201003B12455D53C1816516C5
18493F6398AAFA72B17DFA894DB888A7D48C0A47F62579A4E644F86DA711FEC850CDD9DBBD17F69A44
3D2EC1DD60D3C618FA74CDE5FDAFABD6BAA26EB0A3ADB4DEF6480FB1218CD3B083E252E885B6F0729F
98B2144D2B72293E1B11D73393BC41F75B15EE3D7569B4995ED1A14425DA4319B7B26B0E8FEF17C375
42AE5C6D5849F87209567F3925A47B016D564859717BC57FCB4522D0AA49CE816E5BE7B3088193236E
C9EFFF140858045B73C5D79BAF38F7C67F04C5DCF0E3806AD982D1259058C3473E847179A878F2C6B3
BD968FB99EA46E9185892F3676E78965C2AED4877BA3917DF07C5E927474F19E764BA61DC38D63BF29
02818100D5C69C8C3CDC2464744A793713DAFB9F1DBC799FF96423FECD3CBA794286BCE920F4B5C183
F99EE9028DB6212C6277C4C8297FCFBCE7F7C24CA4C51FC7182FB8F4019FB1D5659674C5CBE6D5FA99
2051341760CD00735729A070A9E54D342BEBA8EF47EE82D3A01B04CEC4A00D4DDB41E35116FC221E85
4B43A696C0E6419B1B02818100CD5EA7702789064B673540CBFF09356AD80BC3D592812EBA47610B9F
AC6AECEFE22ACAE438459CDA74E59653D88C04189D34399BF5B14B920E34EF38A7D09FE69593396E8F
E735E6F0A6AE4990401041D8A406B6FD86A1161E45F95A3EAA5C1012E6662E44F15F335AC971E1766B
2BB9C985109974141B44D37E1E319820A55F02818100B2871237BF9FAD38C3316AB7877A6A868063E5
42A7186D431E8D27C19AC0414584033942E9FF6E2973BB7B2D8B0E94AD1EE82158108FBC8664517A5A
467FB963014BD5DCC2B4FB087C23039D11920DBE22FD9F16B4D89E23225CD455ADBAF32EF43F185864
A36D630309D6853F7714B39AAE1EBEE3938F87C2707E178C739F9F028181009690BED14B2AFAA26D98
6D592231EE27D71D49065BD2BA1F78157E20229881FD9D23227D0F8479EAEFA922FD75D5B16B1A561F
A6680B040CA0BDCE650B23B917A4B1BB7983A74FAD70E1C305CBEC2BFF1A85A726A1D90260E4F1084F
518234DCD3FE770B9520215BD543BB6A4117718754676A34171666A79F26E79C149C5AA102818100A0
C985A0A0A791A659F99731134C44F37B2E520A2CEA35800AD27241ED360DFDE6E8CA614F12047FD08B
76AC4D13C056A0699E2F98A1CAC91011294D71208F4ABAB33BA87AA0517F415BACA88D6BAC006088FA
601D349417E1F0C9B23AFFA4D496618DBC024986ED690BBB7B025768FF9DF8AC15416F489F8129C323
41A8B44F

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000800 (2048)



42007B01000005C042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A556C42000D020000000040000
00010000000042000F010000056842005C0500000004000000000A000000000042007F050000000040000000
00000000000042007C010000054042005705000000040000000400000000420094070000002437636635
323039622D366666362D343432362D383939652D3232623036373835393337320000000004200640100
0004F842004001000004F04200420500000004000000030000000042004501000004B8420043080000
04A9308204A502010002820101000AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF
1E440AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D
7DC7EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795
A41100F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0EC
C8295353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F01
3DA809E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F9
9374FE30E54951662A6EDA29C6FC411335D5DC7426B0F6050203010001028201003B12455D53C18165
16C518493F6398AAFA72B17DFA894DB888A7D48C0A47F62579A4E644F86DA711FEC850CDD9DBBD17F6
9A443D2EC1DD60D3C618FA74CDE5FDAFABD6BAA26EB0A3ADB4DEF6480FB1218CD3B083E252E885B6F0
729F98B2144D2B72293E1B11D73393BC41F75B15EE3D7569B4995ED1A14425DA4319B7B26B0E8FEF17
C37542AE5C6D5849F87209567F3925A47B016D564859717BC57FCB4522D0AA49CE816E5BE7B3088193
236EC9EFFF140858045B73C5D79BAF38F7C67F04C5DCF0E3806AD982D1259058C3473E847179A878F2
C6B3BD968FB99EA46E9185892F3676E78965C2AED4877BA3917DF07C5E927474F19E764BA61DC38D63
BF2902818100D5C69C8C3CDC2464744A793713DAFB9F1DBC799FF96423FECD3CBA794286BCE920F4B5
```

	C183F99EE9028DB6212C6277C4C8297FCFBCE7F7C24CA4C51FC7182FB8F4019FB1D5659674C5CBE6D5 FA992051341760CD00735729A070A9E54D342BEBA8EF47EE82D3A01B04CEC4A00D4DDB41E35116FC22 1E854B43A696C0E6419B1B02818100CD5EA7702789064B673540CBFF09356AD80BC3D592812EBA4761 0B9FAC6AECEFE22ACAE438459CDA74E59653D88C04189D34399BF5B14B920E34EF38A7D09FE6959339 6E8FE735E6F0A6AE4990401041D8A406B6FD86A1161E45F95A3EAA5C1012E6662E44F15F335AC971E1 766B2BB9C985109974141B44D37E1E319820A55F02818100B2871237BF9FAD38C3316AB7877A6A8680 63E542A7186D431E8D27C19AC0414584033942E9FF6E2973BB7B2D8B0E94AD1EE82158108FBC866451 7A5A467FB963014BD5DCC2B4FB087C23039D11920DBE22FD9F16B4D89E23225CD455ADBAF32EF43F18 5864A36D630309D6853F7714B39AAE1EBEE3938F87C2707E178C739F9F028181009690BED14B2AFAA2 6D986D592231EE27D71D49065BD2BA1F78157E20229881FD9D23227D0F8479EAEFA922FD75D5B16B1A 561FA6680B040CA0BDCE650B23B917A4B1BB7983A74FAD70E1C305CBEC2BFF1A85A726A1D90260E4F1 084F518234DCD3FE770B9520215BD543BB6A4117718754676A34171666A79F26E79C149C5AA1028181 00A0C985A0A0A791A659F99731134C44F37B2E520A2CEA35800AD27241ED360DFDE6E8CA614F12047F D08B76AC4D13C056A0699E2F98A1CAC91011294D71208F4ABAB33BA87AA0517F415BACA88D6BAC0060 88FA601D349417E1F0C9B23AFFA4D496618DBC024986ED690BBB7B025768FF9DF8AC15416F489F8129 C32341A8B44F000000000000004200280500000004000000040000000042002A020000000400000800 00000000
6	Get (public key) In: uuidPublicKey, keyFormatType='00000003' Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: 57492708-09e8-4235-ab77-8eee6ed4647f Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000003 (PKCS#1) 42007801000000A0420077010000003842006901000000204200 6A02000000040000000100000000042 006B02000000040000000100000000042000D0200000004000000010000000042000F01000000584200 5C05000000040000000A000000004200790100000040420094070000002435373439323730382D3039 65382D343233352D616237372D3865656536656434363437660000000042004205000000040000000 3 00000000

Out: objectType = ‘00000003’, uuidPublicKey, publicKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556C 
(Fri Apr 27 10:14:36 CEST 2012)
    Tag: 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: 0x00000003 
(Public Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 57492708-
09e8-4235-ab77-8eee6ed4647f
      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: 
0x00000003 (PKCS#1)
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 
3082010A0282010100AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E440AFB80
B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7EC114F
3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA
214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C7
95328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1
B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E5
4951662A6EDA29C6FC411335D5DC7426B0F6050203010001
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 
0x00000004 (RSA)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 
0x00000800 (2048)
```

```
42007B010000022042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A556C42000D0200000040000
```

	00010000000042000F01000001C842005C0500000004000000000A000000000042007F0500000004000000000000000042007C01000001A042005705000000040000000300000000420094070000002435373439323730382D303965382D343233352D616237372D38656565366564343634376600000000042006D01000001584200400100000150420042050000000400000003000000004200450100000118420043080000010E3082010A0282010100AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E440AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E54951662A6EDA29C6FC411335D5DC7426B0F6050203010001000042002805000000040000000040000000042002A0200000004000000800000000000

7	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: 0x00000001 (1)
	    Tag: 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: 7cf5209b-6ff6-4426-899e-22b067859372
	42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000010000000042000D0200000004000000010000000042000F010000004842005C0500000004000000140000000042007901000000304200940700000024376366353230396 22D366666362D343432362D383939652D32326230363738353933373200000000
	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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556C 
(Fri Apr 27 10:14:36 CEST 2012)

    Tag: 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: 7cf5209b-
6ff6-4426-899e-22b067859372



42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B020000000400000001000000004200920900000008000000004F9A556C42000D020000000400000
00010000000042000F010000005842005C050000000400000014000000042007F0500000004000000
000000000042007C0100000030420094070000002437636635323039622D366666362D343432362D38
3939652D32326230363738353933373200000000
```

8

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: 
0x00000001 (1)

    Tag: 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: 57492708-
09e8-4235-ab77-8eee6ed4647f
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000001400000000420079010000003042009407000000243537343932373038 2D3039
65382D343233352D616237372D38656565366564343634376600000000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556C
(Fri Apr 27 10:14:36 CEST 2012)
    Tag: 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: 57492708-
09e8-4235-ab77-8eee6ed4647f
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A556C42000D020000000400000
00010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000
0000000000042007C01000000304200940700000024353734393237303 82D303965382D343233352D61
6237372D38656565366564343634376600000000
```

13.2 Test Case: Register an Asymmetric Key Pair and a Corresponding X.509 Certificate

Register a public/private key pair in the PKCS#1 key format and a corresponding X.509 certificate. Make sure the certificate was registered and the attributes set correctly by listing and retrieving the attributes. Get the keys and certificate, and finally destroy all the registered objects.

This test case is aimed at exercising the functionality defined in the Basic Asymmetric Key and Certificate Store Profile [KMIP-Spec]

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof].

Time	Request/Response messages

0	Register (Public Key)
	In: objectType='00000003', attributes={ CryptographicUsageMask='00000002' }, publicKey
	`Tag: Request Message (0x420078), Type: Structure (0x01), Data:`
	`  Tag: Request Header (0x420077), Type: Structure (0x01), Data:`
	`    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)`
	`    Tag: 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: Public Key (0x42006D), Type: Structure (0x01), Data:

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

          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data:
0x00000003 (PKCS#1)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
3082010A0282010100AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E440AFB80
B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7EC114F
3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA
214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C7
95328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1
B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E5
4951662A6EDA29C6FC411335D5DC7426B0F6050203010001

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000800 (2048)
```

```
42007801000002104200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000001C84200
5C05000000040000000300000000420079010000001B0420057050000000400000003000000000420091
0100000038420008010000003042000A070000001843727970746F677261706869632055736167652 0
4D61736B42000B02000000040000000200000000042006D01000001584200400100000150420042050 0
```

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:
0x00000001 (1)
```

```
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556C
(Fri Apr 27 10:14:36 CEST 2012)

    Tag: 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: cebe88c5-
2f84-4111-bc2c-37a218b16754
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A556C42000D020000000400000
0001000000000042000F01000000058420005C0500000004000000030000000042007F050000000400000
000000000000042007C010000003042009407000000246365626538386335 2D326638342D343131312D62
6332632D3337613231386231363735340000000000
```

1 Register (Private Key)

In: objectType='00000004', attributes={ CryptographicUsageMask='00000001', Link={ LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey } }, privateKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

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

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

    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003
(Register)

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

      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000004
(Private Key)

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

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

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

```
Cryptographic Usage Mask

          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000001
(Sign)

        Tag: 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: cebe88c5-2f84-4111-bc2c-37a218b16754

      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:
0x00000003 (PKCS#1)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
308204A50201000282010100AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E44
0AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7
EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A411
00F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC829
5353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA8
09E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374
FE30E54951662A6EDA29C6FC411335D5DC7426B0F6050203010001028201003B12455D53C1816516C5
18493F6398AAFA72B17DFA894DB888A7D48C0A47F62579A4E644F86DA711FEC850CDD9DBBD17F69A44
3D2EC1DD60D3C618FA74CDE5FDAFABD6BAA26EB0A3ADB4DEF6480FB1218CD3B083E252E885B6F0729F
98B2144D2B72293E1B11D73393BC41F75B15EE3D7569B4995ED1A14425DA4319B7B26B0E8FEF17C375
42AE5C6D5849F87209567F3925A47B016D564859717BC57FCB4522D0AA49CE816E5BE7B3088193236E
C9EFFF140858045B73C5D79BAF38F7C67F04C5DCF0E3806AD982D1259058C3473E847179A878F2C6B3
BD968FB99EA46E9185892F3676E78965C2AED4877BA3917DF07C5E927474F19E764BA61DC38D63BF29
02818100D5C69C8C3CDC2464744A793713DAFB9F1DBC799FF96423FECD3CBA794286BCE920F4B5C183
F99EE9028DB6212C6277C4C8297FCFBCE7F7C24CA4C51FC7182FB8F4019FB1D5659674C5CBE6D5FA99
2051341760CD00735729A070A9E54D342BEBA8EF47EE82D3A01B04CEC4A00D4DDB41E35116FC221E85
4B43A696C0E6419B1B02818100CD5EA7702789064B673540CBFF09356AD80BC3D592812EBA47610B9F
AC6AECEFE22ACAE438459CDA74E59653D88C04189D34399BF5B14B920E34EF38A7D09FE69593396E8F
E735E6F0A6AE4990401041D8A406B6FD86A1161E45F95A3EAA5C1012E6662E44F15F335AC971E1766B
2BB9C985109974141B44D37E1E319820A55F02818100B2871237BF9FAD38C3316AB7877A6A868063E5
42A7186D431E8D27C19AC0414584033942E9FF6E2973BB7B2D8B0E94AD1EE82158108FBC8664517A5A
467FB963014BD5DCC2B4FB087C23039D11920DBE22FD9F16B4D89E23225CD455ADBAF32EF43F185864
A36D630309D6853F7714B39AAE1EBEE3938F87C2707E178C739F9F028181009690BED14B2AFAA26D98
6D592231EE27D71D49065BD2BA1F78157E20229881FD9D23227D0F8479EAEFA922FD75D5B16B1A561F
A6680B040CA0BDCE650B23B917A4B1BB7983A74FAD70E1C305CBEC2BFF1A85A726A1D90260E4F1084F
518234DCD3FE770B9520215BD543BB6A4117718754676A34171666A79F26E79C149C5AA102818100A0
C985A0A0A791A659F99731134C44F37B2E520A2CEA35800AD27241ED360DFDE6E8CA614F12047FD08B
76AC4D13C056A0699E2F98A1CAC91011294D71208F4ABAB33BA87AA0517F415BACA88D6BAC006088FA
601D349417E1F0C9B23AFFA4D496618DBC024986ED690BBB7B025768FF9DF8AC15416F489F8129C323
41A8B44F

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000800 (2048)



420078010000061042007701000000384200690100000020042006A02000000040000000100000000042
```

```
006B02000000040000000100000000042000D02000000040000000100000000042000F01000005C84200
5C05000000040000000300000000420079010000005B04200570500000000400000004000000000420091
01000000984200080100000003042000A070000001843727970746F677261706869632055736167652
4D61736B42000B02000000040000000100000000420008010000005842000A07000000044C696E6B00
00000042000B01000000404200 4B05000000040000010200000000042004C0700000024636562653838
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556C
(Fri Apr 27 10:14:36 CEST 2012)
```

	Tag: 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: 3b094413-2efd-4b54-97df-480eccf2402b 42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420 06B02000000040000000100000000420092090000000800000004F9A556C42000D02000000040000 0001000000004 2000F010000005842005C0500000004000000030000000042007F0500000004000000 000000000042007C010000003042009407000000243362303934343133 2D326566642D346235342D39 3764662D34383065636366323430326200000000
2	Register (Certificate) In: objectType=’00000001’, attributes={ CryptographicUsageMask=‘00000003’, Link={ LinkType=‘PublicKeyLink’, LinkedObjectIdentifier=uuidPublicKey } }, certificate Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: 0x00000001 (Certificate) 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: 0x00000003

```
(Sign, 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: 0x00000102
(Public Key Link)

            Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07),
Data: cebe88c5-2f84-4111-bc2c-37a218b16754

      Tag: Certificate (0x420013), Type: Structure (0x01), Data:

        Tag: Certificate Type (0x42001D), Type: Enumeration (0x05), Data:
0x00000001 (X.509)

        Tag: Certificate Value (0x42001E), Type: Byte String (0x08), Data:
30820312308201FAA003020102020101300D06092A864886F70D0101050500303B310B300906035504
0613025553310D300B060355040A130454455354310E300C060355040B13054F41534953310D300B06
0355040313044B4D4950301E170D3130313130313233353935395A170D3230313130313233353935393539
5A303B310B3009060355040613025553310D300B060355040A130454455354310E300C060355040B13
054F41534953310D300B060355040313044B4D495030820122300D06092A864886F70D010101050003
82010F003082010A0282010100AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E
440AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7D
C7EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A4
1100F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8
295353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013D
A809E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F993
74FE30E54951662A6EDA29C6FC411335D5DC7426B0F6050203010001A321301F301D0603551D0E0416
041404E57BD2C431B2E816E180A19823FAC858273F6B300D06092A864886F70D01010505000382010
100A876ADBC6C8E0FF017216E195FEA76BFF61A567C9A13DC50D13FEC12A4273C441547CFABCB5D61D9
91E966319DF72C0D41BA826A45112FF26089A2344F4D71CF7C921B4BDFAEF1600D1BAAA15336057E01
4B8B496D4FAE9E8A6C1DA9AEB6CBC960CBF2FAE77F587EC4BB282045338845B88DD9AEEA53E482A36E
734E4F5F03B9D0DFC4CAFC6BB34EA9053E52BD609EE01E86D9B09FB51120C19834A997B09CE08D79E8
1311762F974BB1C8C09186C4D78933E0DB38E905084877E147C78AF52FAE07192FF166D19FA94A11CC
11B27ED050F7A27FAE13B205A574C4EE00AA8BD65D0D7057C985C839EF336A441ED53A53C6B6B696F1
BDEB5F7EA811EBB25A7F86



42007801000004484200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000004004200
5C05000000040000000300000000420079010000003E84200570500000004000000010000000420091
01000000984200080100000030420000A070000000184372797074667261706869632055736167652
4D61736B42000B02000000040000000300000000420008010000005842000A07000000044C696E6B00
00000042000B010000004042004B0500000004000001020000000042004C07000000246365626538
63352D326638342D343131312D626332632D333761323138623136373534000000004200130100000003
3042001D05000000040000000100000000042001E080000031630820312308201FAA003020102020101
300D06092A864886F70D0101050500303B310B3009060355040613025553310D300B060355040A1304
54455354310E300C060355040B13054F41534953310D300B060355040313044B4D4950301E170D3130
3131303132333539353935A170D3230313130313233353935395A303B310B300906035504061302555
3310D300B060355040A130454455354310E300C060355040B13054F41534953310D300B060355040313
044B4D495030820122300D06092A864886F70D01010105000382010F003082010A0282010100AB7F16
1C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E440AFB80B64A8755F8002CFEBA6B1845
40A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7EC114F3B176B7957C422E7D03FC626
7FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA214900DF8B65089F98135B1C
67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C795328ABF70E1B42E7BB8B7F4
E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1B7AE64C54130FBC21D80E9C2
CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E54951662A6EDA29C6FC411335
D5DC7426B0F6050203010001A321301F301D0603551D0E0416041404E57BD2C431B2E816E180A19823
FAC858273F6B300D06092A864886F70D01010505000382010100A876ADBC6C8E0FF017216E195FEA76
BFF61A567C9A13DC50D13FEC12A4273C441547CFABCB5D61D991E966319DF72C0D41BA826A45112FF2
6089A2344F4D71CF7C921B4BDFAEF1600D1BAAA15336057E014B8B496D4FAE9E8A6C1DA9AEB6CBC960
```

```
CBF2FAE77F587EC4BB282045338845B88DD9AEEA53E482A36E734E4F5F03B9D0DFC4CAFC6BB34EA905
3E52BD609EE01E86D9B09FB51120C19834A997B09CE08D79E81311762F974BB1C8C09186C4D78933E0
DB38E905084877E147C78AF52FAE07192FF166D19FA94A11CC11B27ED050F7A27FAE13B205A574C4EE
00AA8BD65D0D7057C985C839EF336A441ED53A53C6B6B696F1BDEB5F7EA811EBB25A7F860000
```

Out: uuidCertificate

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556C 
(Fri Apr 27 10:14:36 CEST 2012)
    Tag: 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: 7091d0bf-
548a-4d4a-93a6-6dd71cf75221
```

```
42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042
006B02000000040000000100000000420092090000000800000004F9A556C42000D02000000040000
00010000000042000F010000005842005C050000000400000003000000042007F0500000004000000
000000000042007C0100000030420094070000002437303931643062662D353438612D346434612D39
3361362D3664643731636637353232310000000
```

3

Add attribute

In: uuidPublicKey, attribute={ Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } }

In: uuidPublicKey, attribute={ Link={ LinkType='CertificateLink', LinkedObjectIdentifier=uuidCertificate } }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    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: Byte String (0x08), Data:
31F81BFB0F0492BD
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: cebe88c5-
2f84-4111-bc2c-37a218b16754
      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: 3b094413-2efd-4b54-97df-480eccf2402b
  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: Byte String (0x08), Data:
BA865701C7837BE2
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: cebe88c5-
2f84-4111-bc2c-37a218b16754
      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: 0x00000101
(Certificate Link)
          Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07),
Data: 7091d0bf-548a-4d4a-93a6-6dd71cf75221
```

```
42007801000001C042007701000000384200690100000020420066A020000000400000001000000042
006B02000000040000000100000000042000D0200000004000000020000000042000F01000000B84200
5C050000000040000000D000000004200930800000000831F81BFB0F0492BD420079010000009042009
4070000002463656265383863352D326638342D343131312D626332632D333761323138623136373534
000000004200080100000058420000A07000000044C696E6B000000000042000B01000000404200
4B0500000000400000103000000000420004C07000000243362303934343133322D326566642D346235342D393764
662D34383065636366323430326200000000042000F01000000B842005C0500000000400000000D000000
004200930800000008BA865701C7837BE24200790100000009042009407000000246365626538386335
2D326638342D343131312D626332632D333761323138623136373534000000000420008010000005842
000A0700000044C696E6B0000000042000B01000000404200 4B050000000040000010100000000004200
4C070000002437303931643062662D353438612D346434612D393361362D36646437316366373532 32
3100000000
```

Out: uuidPublicKey, attribute={ Link={ LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey } }

Out: uuidPublicKey, attribute={ Link={ LinkType='CertificateLink', LinkedObjectIdentifier=uuidCertificate } }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556C
(Fri Apr 27 10:14:36 CEST 2012)

    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: Byte String (0x08), Data:
31F81BFB0F0492BD

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: cebe88c5-
2f84-4111-bc2c-37a218b16754

      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: 3b094413-2efd-4b54-97df-480eccf2402b 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: Byte String (0x08), Data: BA865701C7837BE2 Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: cebe88c5-2f84-4111-bc2c-37a218b16754 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link Tag: Attribute Index (0x420009), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000101 (Certificate Link) Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: 7091d0bf-548a-4d4a-93a6-6dd71cf75221 42007B01000002004 2007A0100000048420069010000002042006A02000000040000000100000000420 06B02000000040000000100000000420092090000000800000004F9A556C42000D020000000400000 002000000000042000F01000000C842005C0500000004000000 0D00000000420093080000000831F81B FB0F0492BD42007F050000000400000000000000004 2007C01000000904200940700000024636562653 83863352D326638342D343131312D626332632D3337613231386231363735340000000042000801000 0005842000A07000000044C696E6B000000000 42000B01000000404 2004B05000000040000010300000000 42004C07000000243362303934343133 2D326566642D346235342D393764662D343830656363663234303262000000000 42000F01000000D842005C050000000400000 00D000000004200930800000008 BA865701C7837BE242007F0500000004000000000000000042007C01000000A04200940700000024 63656265383863352D326638342D343131312D626332632D33376132313862313637353400000000 4200080100000068 42000A07000000044C696E6B00000000420009020000000400000001000000004 2000B010000004042004B050000000400000101000000004 2004C0700000024373039316430626 62D353438612D346434612D393361362D366464373163663735323231 00000000
4	Get Attribute List In: uuidCertificate Tag: Request Message (0x420078), Type: Structure (0x01), Data:

```
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: 7091d0bf-
548a-4d4a-93a6-6dd71cf75221
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C0500000004000000C000000004200790100000030420094070000002437303931643062662D3534
38612D346434612D393361362D36646437316366373532323100000000
```

Out: uuidCertificate, attributesNames={ * }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556C 
(Fri Apr 27 10:14:36 CEST 2012)
    Tag: 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: 7091d0bf-548a-4d4a-93a6-6dd71cf75221

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

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

      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: X.509 Certificate Identifier

      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: X.509 Certificate Issuer

      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: X.509 Certificate Subject

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

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

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

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

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

      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: Link

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

      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: 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
```

```
42007B01000002D042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A556C42000D02000000040000
0001000000000042000F010000027842005C0500000004000000C000000000042007F0500000004000000
0000000000042007C010000025042009407000000243730393164306266D353438612D34643461 2D39
3361362D36646437316366373532323100000000042000A0700000014437279707467726170686963
204C656E677468000000000042000A070000001243657274696669636174652 04C656E677468000000
000042000A070000001C582E35303920436572746966696361746520496465 6E74696669657200000
0042000A0700000018582E3530392043657274696669636174652049737375657242000A0700000019
582E35303920436572746966696361746520537562 6A656374000000000000000042000A070000001B44
69676974616C205369676E617475726520416C676F726974686D000000000042000A07000000124365
```

```
727469666963617465204973737565720000000000000042000A07000000104365727469666963617465
205479706542000A0700000013436572746966696361746520537562A6563740000000000042000A07
00000016436572746966696361746520496456E74696669657200042000A0700000005537461 7465
00000042000A07000000064469676573740000042000A07000000044C696E6B000000042000A070000
000A4C65617365205469 6D6500000000000042000A070000000C496E697469616C204461746500000 0
0042000A0700000011556E6971756520496456E7469666965720000000000000042000A0700000018
43727970746F6772617068696320557361676520 4D61736B42000A070000000B4F626A656374205479
706500000000000042000A07000000104C61737420436861E67652044617465
```

5

Get Attributes

In: uuidCertificate, attributesNames={'Certificate Identifier', 'Certificate Issuer', 'Certificate Subject', 'Certificate Type'}

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: 7091d0bf-
548a-4d4a-93a6-6dd71cf75221
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate 
Identifier
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate 
Issuer
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate 
Subject
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate 
Type
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digital 
Signature Algorithm
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: 
Cryptographic Length
```

```
42007801000001504200770100000038420069010000002042006A02000000040000000100000000 42
006B02000000040000000100000000 42000D02000000040000000100000000 42000F01000001084200
```

```
5C05000000040000000B0000000042007901000000F0420094070000002437303931643062662D3534
38612D346434612D393361362D3664643731636637353232310000000042000A070000001643657274
69666963617465204964656E746966696572000042000A070000001243657274696669636174652049
7373756572000000000000000042000A07000000134365727469666963617465205375626A656374000000
000042000A070000001043657274696669636174652054797065420000A070000001B4469676974616C
205369676E617475726520416C676F726974686D000000000042000A07000000144372797074F6772
6170686963204C656E67746800000000
```

Out: uuidCertificate, 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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556D 
(Fri Apr 27 10:14:37 CEST 2012)

    Tag: 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: 7091d0bf-
548a-4d4a-93a6-6dd71cf75221

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

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

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

          Tag: Issuer (0x42003B), Type: Text String (0x07), Data: 
CN=KMIP,OU=OASIS,O=TEST,C=US

          Tag: Serial Number (0x420087), Type: Text String (0x07), Data: 1

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

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

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

          Tag: Certificate Issuer Distinguished Name (0x420017), Type: Text String
```

	(0x07), Data: CN=KMIP,OU=OASIS,O=TEST,C=US Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate Subject Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Certificate Subject Distinguished Name (0x42001C), Type: Text String (0x07), Data: CN=KMIP,OU=OASIS,O=TEST,C=US Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate Type Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000001 (X.509) Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digital Signature Algorithm Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 0x00000003 (SHA-1 with RSA Encryption (PKCS#1 v1.5)) 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: 0x00000800 (2048) 42007B010000027042007A0100000048420069010000002042006A0200000004000000010000000042 006B02000000040000000100000000420092090000000800000004F9A556D42000D02000000040000 0001000000000042000F010000021842005C0500000004000000000B000000042007F0500000004000000 0000000000042007C01000001F04200940700000024373039316430626622D353438612D346434612D39 3361362D366464373163663735323231000000004200080100000006042000A070000001643657274 69 6669636174652049646566E74696669657200004200B010000003842003B070000001C434E3D4B4D49 502C4F553D4F415349532C4F3D544553542C433D5553000000004200870700000013100000000000000 00420008010000005042000A0700000012436572746966696361746520497373756572000000000000 42000B010000002842001707000001C434E3D4B4D49502C4F553D4F415349532C4F3D544553542C43 3D555300000000420008010000005042000A070000001343657274696669636174652053756 26A6563 7400000000000042000B010000002842001C070000001C434E3D4B4D49502C4F553D4F415349532C4F3D 544553542C433D555300000000420008010000002842000A070000001043657274696669636174 6520 547970 6542000B05000000040000000100000000420008010000003842000A070000001B4469676974 616C205369676E617475726520416C676F726974686D000000000042000B05000000040000000300000 0000420008010000003042000A070000001443727970746F6772617068696320 4C656E677468000000 0042000B02000000040000080000000000
6	Get (private key) In: uuidPrivateKey, keyFormatType='00000003'

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: 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: 3b094413-
2efd-4b54-97df-480eccf2402b

      Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000003
(PKCS#1)



42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000584200
5C05000000040000000A000000004200790100000040420094070000002433623039343431332D3265
66642D346235342D393764662D343830656363663234303262000000004200420500000004000000003
00000000
```

Out: objectType = ‘00000004’, uuidPrivateKey, privateKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556D
(Fri Apr 27 10:14:37 CEST 2012)

    Tag: 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: 0x00000004
(Private Key)

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 3b094413-
2efd-4b54-97df-480eccf2402b

      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:
0x00000003 (PKCS#1)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
308204A50201000282010100AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E44
0AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7
EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A411
00F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC829
5353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA8
09E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374
FE30E54951662A6EDA29C6FC411335D5DC7426B0F6050203010001028201003B12455D53C1816516C5
18493F6398AAFA72B17DFA894DB888A7D48C0A47F62579A4E644F86DA711FEC850CDD9DBBD17F69A44
3D2EC1DD60D3C618FA74CDE5FDAFABD6BAA26EB0A3ADB4DEF6480FB1218CD3B083E252E885B6F0729F
98B2144D2B72293E1B11D73393BC41F75B15EE3D7569B4995ED1A14425DA4319B7B26B0E8FEF17C375
42AE5C6D5849F87209567F3925A47B016D564859717BC57FCB4522D0AA49CE816E5BE7B3088193236E
C9EFFF140858045B73C5D79BAF38F7C67F04C5DCF0E3806AD982D1259058C3473E847179A878F2C6B3
BD968FB99EA46E9185892F3676E78965C2AED4877BA3917DF07C5E927474F19E764BA61DC38D63BF29
02818100D5C69C8C3CDC2464744A793713DAFB9F1DBC799FF96423FECD3CBA794286BCE920F4B5C183
F99EE9028DB6212C6277C4C8297FCFBCE7F7C24CA4C51FC7182FB8F4019FB1D5659674C5CBE6D5FA99
2051341760CD00735729A070A9E54D342BEBA8EF47EE82D3A01B04CEC4A00D4DDB41E35116FC221E85
4B43A696C0E6419B1B02818100CD5EA7702789064B673540CBFF09356AD80BC3D592812EBA47610B9F
AC6AECEFE22ACAE438459CDA74E59653D88C04189D34399BF5B14B920E34EF38A7D09FE69593396E8F
E735E6F0A6AE4990401041D8A406B6FD86A1161E45F95A3EAA5C1012E6662E44F15F335AC971E1766B
2BB9C985109974141B44D37E1E319820A55F02818100B2871237BF9FAD38C3316AB7877A6A868063E5
42A7186D431E8D27C19AC0414584033942E9FF6E2973BB7B2D8B0E94AD1EE82158108FBC8664517A5A
467FB963014BD5DCC2B4FB087C23039D11920DBE22FD9F16B4D89E23225CD455ADBAF32EF43F185864
A36D630309D6853F7714B39AAE1EBEE3938F87C2707E178C739F9F028181009690BED14B2AFAA26D98
6D592231EE27D71D49065BD2BA1F78157E20229881FD9D23227D0F8479EAEFA922FD75D5B16B1A561F
A6680B040CA0BDCE650B23B917A4B1BB7983A74FAD70E1C305CBEC2BFF1A85A726A1D90260E4F1084F
518234DCD3FE770B9520215BD543BB6A4117718754676A34171666A79F26E79C149C5AA102818100A0
C985A0A0A791A659F99731134C44F37B2E520A2CEA35800AD27241ED360DFDE6E8CA614F12047FD08B
76AC4D13C056A0699E2F98A1CAC91011294D71208F4ABAB33BA87AA0517F415BACA88D6BAC006088FA
601D349417E1F0C9B23AFFA4D496618DBC024986ED690BBB7B025768FF9DF8AC15416F489F8129C323
41A8B44F

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000800 (2048)



42007B01000005C042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A556D42000D020000000400000
00010000000042000F010000056842005C0500000004000000000A0000000042007F05000000004000000
00000000000042007C0100000540420057050000000400000004000000004200940700000024336230 39
343431332D326566642D346235342D393764662D343830656363663234303262000000004200640100
0004F842004001000004F0420042050000000400000003000000004200450100000 4B842004308000 0
04A9308204A50201000282010100AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF
1E440AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D
7DC7EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795
```

```
A41100F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0EC
C8295353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F01
3DA809E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F9
9374FE30E54951662A6EDA29C6FC411335D5DC7426B0F6050203010001028201003B12455D53C18165
16C518493F6398AAFA72B17DFA894DB888A7D48C0A47F62579A4E644F86DA711FEC850CDD9DBBD17F6
9A443D2EC1DD60D3C618FA74CDE5FDAFABD6BAA26EB0A3ADB4DEF6480FB1218CD3B083E252E885B6F0
729F98B2144D2B72293E1B11D73393BC41F75B15EE3D7569B4995ED1A14425DA4319B7B26B0E8FEF17
C37542AE5C6D5849F87209567F3925A47B016D564859717BC57FCB4522D0AA49CE816E5BE7B3088193
236EC9EFFF140858045B73C5D79BAF38F7C67F04C5DCF0E3806AD982D1259058C3473E847179A878F2
C6B3BD968FB99EA46E9185892F3676E78965C2AED4877BA3917DF07C5E927474F19E764BA61DC38D63
BF2902818100D5C69C8C3CDC2464744A793713DAFB9F1DBC799FF96423FECD3CBA794286BCE920F4B5
C183F99EE9028DB6212C6277C4C8297FCFBCE7F7C24CA4C51FC7182FB8F4019FB1D5659674C5CBE6D5
FA992051341760CD00735729A070A9E54D342BEBA8EF47EE82D3A01B04CEC4A00D4DDB41E35116FC22
1E854B43A696C0E6419B1B02818100CD5EA7702789064B673540CBFF09356AD80BC3D592812EBA4761
0B9FAC6AECEFE22ACAE438459CDA74E59653D88C04189D34399BF5B14B920E34EF38A7D09FE6959339
6E8FE735E6F0A6AE4990401041D8A406B6FD86A1161E45F95A3EAA5C1012E6662E44F15F335AC971E1
766B2BB9C985109974141B44D37E1E319820A55F02818100B2871237BF9FAD38C3316AB7877A6A8680
63E542A7186D431E8D27C19AC0414584033942E9FF6E2973BB7B2D8B0E94AD1EE82158108FBC866451
7A5A467FB963014BD5DCC2B4FB087C23039D11920DBE22FD9F16B4D89E23225CD455ADBAF32EF43F18
5864A36D630309D6853F7714B39AAE1EBEE3938F87C2707E178C739F9F028181009690BED14B2AFAA2
6D986D592231EE27D71D49065BD2BA1F78157E20229881FD9D23227D0F8479EAEFA922FD75D5B16B1A
561FA6680B040CA0BDCE650B23B917A4B1BB7983A74FAD70E1C305CBEC2BFF1A85A726A1D90260E4F1
084F518234DCD3FE770B9520215BD543BB6A4117718754676A34171666A79F26E79C149C5AA1028181
00A0C985A0A0A791A659F99731134C44F37B2E520A2CEA35800AD27241ED360DFDE6E8CA614F12047F
D08B76AC4D13C056A0699E2F98A1CAC91011294D71208F4ABAB33BA87AA0517F415BACA88D6BAC0060
88FA601D349417E1F0C9B23AFFA4D496618DBC024986ED690BBB7B025768FF9DF8AC15416F489F8129
C32341A8B44F0000000000000042002805000000040000000400000000420002A020000000400000800
00000000
```

7

Get (public key)

In: uuidPublicKey, keyFormatType='00000003'

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: 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: cebe88c5-
2f84-4111-bc2c-37a218b16754

      Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000003
(PKCS#1)
```

```
42007801000000A04200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000584200
5C05000000040000000A000000004200790100000040420094070000002463656265383863352D3266
38342D343131312D626332632D33376132313862313637353400000000420042050000000400000003
00000000
```

Out: objectType = ‘00000004’, uuidPublicKey, publicKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556D 
(Fri Apr 27 10:14:37 CEST 2012)

    Tag: 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: 0x00000003 
(Public Key)

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: cebe88c5-
2f84-4111-bc2c-37a218b16754

      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: 
0x00000003 (PKCS#1)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 
3082010A0282010100AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E440AFB80
B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7EC114F
3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA
214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C7
95328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1
B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E5
```

```
4951662A6EDA29C6FC411335D5DC7426B0F6050203010001

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 
0x00000800 (2048)
```

```
42007B010000022042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A556D42000D02000000040000
0001000000000042000F01000001C842005C0500000004000000000A000000042007F0500000004000000
0000000000042007C01000001A0420057050000000400000003000000000420094070000002463656265
383863352D326638342D343131312D626332632D33376132313862313637353400000000042006D0100
00015842004001000001504200420500000004000000030000000042004501000001184200430800000
010E3082010A0282010100AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E440A
FB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7EC
114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100
F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC82953
53C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809
E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE
30E54951662A6EDA29C6FC411335D5DC7426B0F605020301000100004200280500000004000000000400
00000042002A02000000040000080000000000
```

8

Get (certificate)

In: uuidCertificate

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data: 
  Tag: Request Header (0x420077), Type: Structure (0x01), Data: 
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: 
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: 7091d0bf-
548a-4d4a-93a6-6dd71cf75221
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000000A00000000420079010000003042009407000000243730393164306262D3534
38612D346434612D393361362D36646437316366373532323100000000
```

Out: objectType = ‘00000001’, uuidCertificate, certificate

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556D
(Fri Apr 27 10:14:37 CEST 2012)
    Tag: 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: 0x00000001
(Certificate)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 7091d0bf-
548a-4d4a-93a6-6dd71cf75221
      Tag: Certificate (0x420013), Type: Structure (0x01), Data:
        Tag: Certificate Type (0x42001D), Type: Enumeration (0x05), Data:
0x00000001 (X.509)
        Tag: Certificate Value (0x42001E), Type: Byte String (0x08), Data:
30820312308201FAA003020102020101300D06092A864886F70D0101050500303B310B300906035504
0613025553310D300B060355040A130454455354310E300C060355040B13054F4153495331 0D300B06
0355040313044B4D4950301E170D3130313130313233353935395A170D32303131303132333539353 9
5A303B310B3009060355040613025553310D300B060355040A130454455354310E300C060355040B13
054F41534953310D300B060355040313044B4D495030820122300D06092A864886F70D010101050003
82010F003082010A0282010100AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E
440AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7D
C7EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A4
1100F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8
295353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013D
A809E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F993
74FE30E54951662A6EDA29C6FC411335D5DC7426B0F6050203010001A321301F301D0603551D0E0416
041404E57BD2C431B2E816E180A19823FAC858273F6B300D06092A864886F70D01010505000382010 1
00A876ADBC6C8E0FF017216E195FEA76BFF61A567C9A13DC50D13FEC12A4273C441547CFABCB5D61D9
91E966319DF72C0D41BA826A45112FF26089A2344F4D71CF7C921B4BDFAEF1600D1BAAA15336057E01
4B8B496D4FAE9E8A6C1DA9AEB6CBC960CBF2FAE77F587EC4BB282045338845B88DD9AEEA53E482A36E
734E4F5F03B9D0DFC4CAFC6BB34EA9053E52BD609EE01E86D9B09FB51120C19834A997B09CE08D79E8
1311762F974BB1C8C09186C4D78933E0DB38E905084877E147C78AF52FAE07192FF166D19FA94A11CC
```

	11B27ED050F7A27FAE13B205A574C4EE00AA8BD65D0D7057C985C839EF336A441ED53A53C6B6B696F1 BDEB5F7EA811EBB25A7F86 42007B01000003F842007A0100000048420069010000002042006A0200000004000000010000000042 006B0200000004000000010000000042009209000000080000000004F9A556D42000D02000000040000 00010000000042000F01000003A042005C050000000400000000A000000042007F0500000004000000 00000000042007C01000003784200570500000004000000010000000042009407000000243730393 1 643062662D353438612D346434612D393361362D3664643731636637353232310000000042001301000 00033042001D0500000004000000010000000042001E080000031630820312308201FAA00302010202 0101300D06092A864886F70D0101050500303B310B3009060355040613025553310D300B060355040A 130454455354310E300C060355040B13054F41534953310D300B060355040313044B4D4950301E170D 3130313130313233353935395A170D3230313130313233353935395A303B310B300906035504061302 5553310D300B060355040A130454455354310E300C060355040B13054F41534953310D300B06035504 0313044B4D495030820122300D06092A864886F70D01010105000382010F003082010A0282010100AB 7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E440AFB80B64A8755F8002CFEBA6B 184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7EC114F3B176B7957C422E7D03F C6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA214900DF8B65089F9813 5B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C795328ABF70E1B42E7BB8 B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1B7AE64C54130FBC21D80 E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E54951662A6EDA29C6FC41 1335D5DC7426B0F6050203010001A321301F301D0603551D0E0416041404E57BD2C431B2E816E180A1 9823FAC858273F6B300D06092A864886F70D01010505000382010100A876ADBC6C8E0FF017216E195F EA76BFF61A567C9A13DC50D13FEC12A4273C441547CFABCB5D61D991E966319DF72C0D41BA826A4511 2FF26089A2344F4D71CF7C921B4BDFAEF1600D1BAAA15336057E014B8B496D4FAE9E8A6C1DA9AEB6CB C960CBF2FAE77F587EC4BB282045338845B88DD9AEEA53E482A36E734E4F5F03B9D0DFC4CAFC6BB34E A9053E52BD609EE01E86D9B09FB51120C19834A997B09CE08D79E81311762F974BB1C8C09186C4D789 33E0DB38E905084877E147C78AF52FAE07192FF166D19FA94A11CC11B27ED050F7A27FAE13B205A574 C4EE00AA8BD65D0D7057C985C839EF336A441ED53A53C6B6B696F1BDEB5F7EA811EBB25A7F860000

9	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: 0x00000001 (1)
	    Tag: 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: 3b094413-2efd-4b54-97df-480eccf2402b

	420078010000009042007701000000384200690100000020 42006A0200000004000000010000000042 006B02000000040000000100000000 42000D0200000004000000010000000042000F01000000484200 5C050000000400000014000000004200790100000030420094070000002433623039343431332D3265 66642D346235342D393764662D343830656363663234303262000000000 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: 0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556D (Fri Apr 27 10:14:37 CEST 2012) Tag: 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: 3b094413-2efd-4b54-97df-480eccf2402b 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042 006B0200000004000000010000000042009209000000080000000004F9A556D42000D020000000040000 00010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000 0000000000042007C0100000030420094070000002433623039343431332D326566642D346235342D39 3764662D343830656363663234303262000000000
10	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: 
0x00000001 (1)

    Tag: 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: cebe88c5-
2f84-4111-bc2c-37a218b16754



42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F010000004842000
5C050000000400000014000000004200790100000030420094070000002463656265383863352D3266
38342D343131312D626332632D33376132313862313637353400000000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556D 
(Fri Apr 27 10:14:37 CEST 2012)

    Tag: 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: cebe88c5-2f84-4111-bc2c-37a218b16754 42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042006B0200000004000000010000000042009209000000080000000004F9A556D42000D0200000004000000010000000042000F010000005842005C05000000040000001400000000042007F05000000040000000000000000042007C010000003042009407000000246365626538386335 2D326638342D343131312D62 6332632D3337613231386231363735340000000
11	Destroy In: uuidCertificate Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: 7091d0bf-548a-4d4a-93a6-6dd71cf75221 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000010000000042000D0200000004000000010000000042000F010000004842005C0500000004000000140000000042007901000000304200940700000024373039316430626 62D353438612D346434612D393361362D366464373163663735323231000000000 Out: uuidCertificate Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data:

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556D 
(Fri Apr 27 10:14:37 CEST 2012)

    Tag: 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: 7091d0bf-
548a-4d4a-93a6-6dd71cf75221



42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A556D42000D020000000400000
0001000000042000F010000005842005C050000000400000014000000000042007F0500000004000000
00000000042007C010000003042009407000000243730393164306266 2D353438612D346434612D39
3361362D366464373163663735323231 00000000
```

13.3 Test Case: Create, Re-key Key Pair

Create a public/private key pair on the server and retrieve the keys in PKCS#1 format. Re-key the key pair and retrieve the new public/private key pair in transparent format. To verify that the links are set correctly, the Link attributes are retrieved. Finally, all the keys are destroyed.

This test case is aimed at exercising the functionality defined in the Basic Asymmetric Key Foundry and Server Profile [KMIP-Spec]

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof].

Time	Request/Response messages
0	Create Key-pair In: commonAttributes={ CryptographicAlgorithm='00000004', CryptographicLength=2048 }, privateKeyAttributes={ Name='PrivateKey1', CryptographicUsageMask=‘00000001’ }, publicKeyAttributes={ Name='PublicKey1', 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: 0x00000001 (1)
    Tag: 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: 0x00000800 (2048)
      Tag: Private Key Template-Attribute (0x420065), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: PrivateKey1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 (Uninterpreted Text String)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000001 (Sign)
      Tag: Public Key Template-Attribute (0x42006E), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: PublicKey1
            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001
(Uninterpreted Text String)
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data:
Cryptographic Usage Mask
          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000002
(Verify)
```

```
42007801000001E84200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420000D020000000400000001000000000042000F01000001A04200
5C050000000400000002000000004200790100000188842001F0100000070420008010000003042000A
07000000174372797074466F677261706869632041C676F726974686D0042000B050000000400000004
00000000420008010000003042000A070000001443727970746F6772617068696320C656E67746800
00000042000B02000000040000080000000000420065010000008042000801000000404200A070000
00044E616D650000000042000B010000002842005507000000B50726976617465B65793100000000
0042005405000000040000000100000000420008010000003042000A07000000184372797074F6772
61706869632055736167652044D61736B42000B02000000040000000100000000042006E010000008042
000801000000404200A07000000044E616D650000000042000B010000002842005507000000A5075
626C69634B6579310000000000004200540500000004000000010000000042000801000003042000A
07000000184372797074F6772617068696320557361676520444D61736B42000B020000000400000002
00000000
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556F
(Fri Apr 27 10:14:39 CEST 2012)
    Tag: 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: Private Key Unique Identifier (0x420066), Type: Text String (0x07), Data: bbc58640-9ff2-4f8d-8a0f-8d977e1cc12c Tag: Public Key Unique Identifier (0x42006F), Type: Text String (0x07), Data: 9f5e2833-2df0-400d-9414-74ce8a4b9dee 42007B01000000E042007A0100000048420069010000002042006A02000000040000000100000000042 006B02000000040000000100000000420092090000000800000004F9A556F42000D020000000400000 0001000000000042000F01000000884200 5C050000000400000002000000000042007F0500000004000000 00000000000042007C01000000604200660700000024626263353836343020D396666322D346638642D38 6130662D38643937376531636331326300000000042006F0700000024396635653238333332D32646630 2D343030642D393431342D3734636538613462396465650000000

1	Get (private key)
	In: uuidPrivateKey, keyFormatType='00000003'
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
	    Tag: 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: bbc58640-9ff2-4f8d-8a0f-8d977e1cc12c
	      Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000003 (PKCS#1)
	
	42007801000000A042007701000000384200690100000020 42006A02000000040000000100000000042
	006B02000000040000000100000000042000D02000000040000000100000000042000F01000000584200
	5C0500000004000000A0000000042007901000000404200940700000024626263353836343020D3966
	66322D346638642D386130662D38643937376531636331326300000000420042050000000400000003
	00000000

Out: uuidPrivateKey, privateKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556F 
(Fri Apr 27 10:14:39 CEST 2012)

    Tag: 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: 0x00000004 
(Private Key)

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: bbc58640-
9ff2-4f8d-8a0f-8d977e1cc12c

      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: 
0x00000003 (PKCS#1)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 
308204A30201000282010100B0612BCCAFDD11D41819A274526D68DBF3C3F25667C402A0E0E8E4CCE0
07EA6B6EA53699E8BD7CCAB7D5AE66C00B28FD678B81BA1D4E841C3A36CAF13F852004633F80D840BE
7AAD9BCDEABDE11514B6AB3BCE602E11305CF5E9C34EBEE32C3C468B9B146502738C0AE82E63AB8BD1
FC4DB0C6A09EB0C9F6E01B9CC8D22317AEDAB328209A1DC5D2CE8529D81521C41730C1C8C76249D233
E89096CA44DFEB469E3532BB90D6691C6932D0C63DBB7647C6E64337B719A1F100B1366CFF3BBB213B
17C716BEB2C9AD88B3B76ABACC378C4898636480FFF1108E1FA1E7573C096606E21B18A05245EBD976
701BB676DC2962A328D39385EF7571BC48AE134B37410203010001028201003 7B71A3CD838BF0EFE65
EA9950085B9D4F4D5059D70165CB2800A975C636F9E7E1D5B27FBFB34B9E459FEC2D6CF0998C228F40
F567988BC6D6E4C40A9D04126F1062D8F276D134B36E8A0762DF9CE72424C70993FC3955CBA7AAA615
53DB32F7FF58CE2E0D124F29A7B05C2703E370FB80171D47539988D2C14C37A4802CB1A7F5685BCC78
865480CA4E5D367CAFC8B533E610620F94F54A082EFFC4C4E50998410DD32FA7DEDAE895200B56437F
E177F47D1B373B5E8E0C62F64B3A19E5918BE83E90A1BBE195A4B516F3CEAE6DB35B0E4427858631DC
BCE6B1E49CF12345297DF41E54D2CBC2834C34E37BB92888E4659D232A4F3D22EDEB9BFF43B7881C79
02818100EAB386180DEC393C70C8B00C5FAE6A10E6B620AE82E5096CE11BF4C539A015165A7481227E
91492748159D85317D1E81B780CCA1CF19630A10987B940663A2496A4EAD2ED4BFB7017DC813E7A490
```

```
17AA278B8AC1381EF27FDE54ED4A1EE1E74812DCAEE514CB9D48590EB3972B26BA2F21DE0AAB64CFC1
DBCBA32561F5F31D6F02818100C062BE5756E93EBE005BE752A5B7BE2D35B342E483FF266CC9F595ED
BCFFFF603C8E03DCD9350A19FABF434077F9543088132F0E843C2DA6FE4F1CEDEE49A5EB9A8AEA1219
A41C1DB39252196137A041DEF9EDCFF43AA9280D90BE137DBF48777E6055695F58FCC9CD6B07924FDA
B47A5553F5AD7B82D52553F6EC3F647FFE4F0281804221676D2BAF1DC97BF5F034EC58D6A6007BDCE5
8F183DF9A1CC20C1D9A4D38C42DC84EE553F569F6CDE3A4E274D9BE4ECF1ABB70405A1345ACCBC354F
3F8FA0A4059B2290EB9C031D8FDC9BEE70735A8C5DF330D241560ED574948FC7F7DB1521CB70B43791
CFB56CF28983D4B2CACF30F9C183DD99F4839BF3523B31F3D89D0281806CBE63C0928BBCBF410CB1B0
71A36E87B776E034B2B7A24C93CB913794414F64625613B0DDC5B134061BDE33AE9CEC0D929CE5585B
3E78BF8FB7C02E6D268BF6A4A028B69A6FBCC4BD1FD3F02C9778AA43131A6D152BA339D491201F7C50
86F1A429679DEC1B2CA814C88EBB11101A3B9BC79D72B601B9E12398CAE8FA31AED90281810099777C
D45F0D1A862888EB2CF7AC14D22D75B88E99ADF66F15CCCBD29979BF5EAA90BB8C29B29A8BE1257425
A9A2DB2F493DF4A740C7FBC138E4B4D80F24E7CA11D63528D900BA2DD5C44DA59E2D601544EC926811
61F17B86C838694A49A978F76FF05287BFCE0704C6F3F9FA87551D0CF1A970B2CB130B5320783A36EA
8613

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000800 (2048)
```

```
42007B01000005B842007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A556F42000D02000000040000
0001000000000042000F010000056042005C0500000004000000A000000042007F0500000004000000
00000000042007C010000053842005705000000040000000400000004200940700000002462626335
383634302D396666322D346638642D386130662D38643937376531636331326300000000420064010
0004F042004001000004E8420042050000000400000003000000004200450100004B0420043080000
04A7308204A302010002820101 00B0612BCCAFDD11D41819A274526D68DBF3C3F25667C402A0E0E8E4
CCE007EA6B6EA53699E8BD7CCAB7D5AE66C00B28FD678B81BA1D4E841C3A36CAF13F852004633F80D8
40BE7AAD9BCDEABDE11514B6AB3BCE602E11305CF5E9C34EBEE32C3C468B9B146502738C0AE82E63AB
8BD1FC4DB0C6A09EB0C9F6E01B9CC8D22317AEDAB328209A1DC5D2CE8529D81521C41730C1C8C76249
D233E89096CA44DFEB469E3532BB90D6691C6932D0C63DBB7647C6E64337B719A1F100B1366CFF3BBB
213B17C716BEB2C9AD88B3B76ABACC378C4898636480FFF1108E1FA1E7573C096606E21B18A05245EB
D976701BB676DC2962A328D39385EF7571BC48AE134B374102030100010282010037B71A3CD838BF0E
FE65EA9950085B9D4F4D5059D70165CB2800A975C636F9E7E1D5B27FBFB34B9E459FEC2D6CF0998C22
8F40F567988BC6D6E4C40A9D04126F1062D8F276D134B36E8A0762DF9CE72424C70993FC3955CBA7AA
A61553DB32F7FF58CE2E0D124F29A7B05C2703E370FB80171D47539988D2C14C37A4802CB1A7F5685B
CC78865480CA4E5D367CAFC8B533E610620F94F54A082EFFC4C4E50998410DD32FA7DEDAE895200B56
437FE177F47D1B373B5E8E0C62F64B3A19E5918BE83E90A1BBE195A4B516F3CEAE6DB35B0E44278586
31DCBCE6B1E49CF12345297DF41E54D2CBC2834C34E37BB92888E4659D232A4F3D22EDEB9BFF43B788
1C7902818100EAB386180DEC393C70C8B00C5FAE6A10E6B620AE82E5096CE11BF4C539A015165A7481
227E91492748159D85317D1E81B780CCA1CF19630A10987B940663A2496A4EAD2ED4BFB7017DC813E7
A49017AA278B8AC1381EF27FDE54ED4A1EE1E74812DCAEE514CB9D48590EB3972B26BA2F21DE0AAB64
CFC1DBCBA32561F5F31D6F02818100C062BE5756E93EBE005BE752A5B7BE2D35B342E483FF266CC9F5
95EDBCFFFF603C8E03DCD9350A19FABF434077F9543088132F0E843C2DA6FE4F1CEDEE49A5EB9A8AEA
1219A41C1DB39252196137A041DEF9EDCFF43AA9280D90BE137DBF48777E6055695F58FCC9CD6B0792
4FDAB47A5553F5AD7B82D52553F6EC3F647FFE4F0281804221676D2BAF1DC97BF5F034EC58D6A6007B
DCE58F183DF9A1CC20C1D9A4D38C42DC84EE553F569F6CDE3A4E274D9BE4ECF1ABB70405A1345ACCBC
354F3F8FA0A4059B2290EB9C031D8FDC9BEE70735A8C5DF330D241560ED574948FC7F7DB1521CB70B4
3791CFB56CF28983D4B2CACF30F9C183DD99F4839BF3523B31F3D89D0281806CBE63C0928BBCBF410C
B1B071A36E87B776E034B2B7A24C93CB913794414F64625613B0DDC5B134061BDE33AE9CEC0D929CE5
585B3E78BF8FB7C02E6D268BF6A4A028B69A6FBCC4BD1FD3F02C9778AA43131A6D152BA339D491201F
7C5086F1A429679DEC1B2CA814C88EBB11101A3B9BC79D72B601B9E12398CAE8FA31AED90281810099
777CD45F0D1A862888EB2CF7AC14D22D75B88E99ADF66F15CCCBD29979BF5EAA90BB8C29B29A8BE125
7425A9A2DB2F493DF4A740C7FBC138E4B4D80F24E7CA11D63528D900BA2DD5C44DA59E2D601544EC92
681161F17B86C838694A49A978F76FF05287BFCE0704C6F3F9FA87551D0CF1A970B2CB130B5320783A
36EA86130042002805000000040000000400000000042002A0200000004000008000000000
```

2	Get (public key)

In: uuidPublicKey, keyFormatType='00000003'

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: 9f5e2833-
2df0-400d-9414-74ce8a4b9dee
      Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000003 
(PKCS#1)
```

```
42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000584200
5C05000000040000000A000000004200790100000040420094070000002439663565323833332D3264
66302D343030642D393431342D373463653861346239646565000000004200420500000004000000003
00000000
```

Out: uuidPublicKey, publicKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A556F 
(Fri Apr 27 10:14:39 CEST 2012)
```

	Tag: 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: 0x00000003 (Public Key) Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 9f5e2833-2df0-400d-9414-74ce8a4b9dee 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: 0x00000003 (PKCS#1) Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 3082010A0282010100B0612BCCAFDD11D41819A274526D68DBF3C3F25667C402A0E0E8E4CCE007EA6B 6EA53699E8BD7CCAB7D5AE66C00B28FD678B81BA1D4E841C3A36CAF13F852004633F80D840BE7AAD9B CDEABDE11514B6AB3BCE602E11305CF5E9C34EBEE32C3C468B9B146502738C0AE82E63AB8BD1FC4DB0 C6A09EB0C9F6E01B9CC8D22317AEDAB328209A1DC5D2CE8529D81521C41730C1C8C76249D233E89096 CA44DFEB469E3532BB90D6691C6932D0C63DBB7647C6E64337B719A1F100B1366CFF3BBB213B17C716 BEB2C9AD88B3B76ABACC378C4898636480FFF1108E1FA1E7573C096606E21B18A05245EBD976701BB6 76DC2962A328D39385EF7571BC48AE134B37410203010001 Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000004 (RSA) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000800 (2048) 42007B010000022042007A0100000048420069010000002042006A0200000004000000010000000042 006B02000000040000000100000000420092090000000800000004F9A556F42000D020000000400000 0001000000000042000F01000001C842005C0500000004000000A0000000042007F0500000004000000 0000000000042007C01000001A042005705000000040000000300000000420094070000002439663565 323833332D326466302D343030642D393431342D373463653861346239646565000000000042006D0100 000158420040010000015042004205000000040000000300000000420045010000011842004308000 0 010E3082010A0282010100B0612BCCAFDD11D41819A274526D68DBF3C3F25667C402A0E0E8E4CCE007 EA6B6EA53699E8BD7CCAB7D5AE66C00B28FD678B81BA1D4E841C3A36CAF13F852004633F80D840BE7A AD9BCDEABDE11514B6AB3BCE602E11305CF5E9C34EBEE32C3C468B9B146502738C0AE82E63AB8BD1FC 4DB0C6A09EB0C9F6E01B9CC8D22317AEDAB328209A1DC5D2CE8529D81521C41730C1C8C76249D233E8 9096CA44DFEB469E3532BB90D6691C6932D0C63DBB7647C6E64337B719A1F100B1366CFF3BBB213B17 C716BEB2C9AD88B3B76ABACC378C4898636480FFF1108E1FA1E7573C096606E21B18A05245EBD97670 1BB676DC2962A328D39385EF7571BC48AE134B3741020301000100004200280500000004000000 0400 00000042002A02000000040000080000000000
3	Re-key Key Pair 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: 
0x00000001 (1)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001D (Re-key 
Key Pair)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Private Key Unique Identifier (0x420066), Type: Text String (0x07), 
Data: bbc58640-9ff2-4f8d-8a0f-8d977e1cc12c
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000001D000000004200790100000030420066070000002462626335383634302D3966
66322D346638642D386130662D38643937376531636331326300000000
```

Out: uuidRekeyedPrivateKey, uuidRekeyedPublicKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571 
(Fri Apr 27 10:14:41 CEST 2012)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001D (Re-key 
Key Pair)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 
(Success)
```

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

      Tag: Private Key Unique Identifier (0x420066), Type: Text String (0x07), 
Data: fbee2a69-e36e-4dce-bb80-b68b5668ec7e

      Tag: Public Key Unique Identifier (0x42006F), Type: Text String (0x07), 
Data: d61b7a14-6204-4272-bae5-1430dd2b6cba
```

```
42007B01000000E042007A0100000048420069010000002042006A02000000040000000100000000042
006B020000000400000001000000004200920900000008000000004F9A557142000D020000000400000
0001000000000042000F01000000088420005C050000000400000001D00000000042007F050000000400000
000000000042007C0100000060420066070000002466626565326136392D653336652D346463652D62
6238302D62363862353636386563376500000000042006F0700000024643631623761342D36323034
2D343237322D626165352D3134333064643262366362610000000
```

4

Locate and Get (private key by name)

In (header): batchOrderOption='TRUE'

In: attributes={ Name={ Name='PrivateKey1', NameType='00000001'}, objectType = '00000004' }

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: 
0x00000001 (1)

    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: Byte String (0x08), Data: 
F409F9ADC43F836F

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

      Tag: Maximum Items (0x42004F), Type: Integer (0x02), Data: 0x00000001 (1)

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

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

        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Name Value (0x420055), Type: Text String (0x07), Data: PrivateKey1

          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 
(Uninterpreted Text String)

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

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

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
396C4D8B5BDE0667

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

      Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x0000000A 
(Transparent RSA Private Key)
```

```
42007801000001484200770100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200100600000008000000000000000142000D02000000040000
00020000000042000F01000000B042005C050000000400000008000000004200930800000008F409F9
ADC43F836F42007901000000884200 4F020000000400000001000000004200080100000040 42000A07
000000044E616D650000000042000B010000002842005507000000 0B507269766174654B6579310000
0000004200540500000004000000010000000042000801000000 2842000A070000000B4F626A656374
2054797065000000000042000B05000000040000000400000000 42000F010000003842005C05000000
040000000A000000004200930800000008396C4D8B5BDE066742007901000000104200420500000004
0000000A00000000
```

Out: uuidRekeyedPrivateKey

Out: rekeyedPrivateKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571 
(Fri Apr 27 10:14:41 CEST 2012)

    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: Byte String (0x08), Data:
F409F9ADC43F836F

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbee2a69-
e36e-4dce-bb80-b68b5668ec7e

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
396C4D8B5BDE0667

    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: 0x00000004
(Private Key)

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: fbee2a69-
e36e-4dce-bb80-b68b5668ec7e

      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:
0x0000000A (Transparent RSA Private Key)

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

            Tag: Key Material (0x420043), Type: Structure (0x01), Data:

              Tag: Modulus (0x420052), Type: Big Integer (0x04), Data:
0000000000000000EAB4492BBB2364359408C57B8AF47003572C81AAED719ED92D9B13C741CC196B71
7D1C98F0C250580E37AC3ADE11A7CD1AAEDE3A0424B53D33200510CE7EEF71DED7E96E585D1D7BA376
7A8DBFAD4D2701B5831A34552A827FC2CD398E659FD5063E1DFD28A994B0E6A7449BBAD8DCF40E2294
3B841AA9E58519FA3575B4409ABFEB57F5723B45F7CE4E5277A2D0ACCCBCD49608D6FF8A7C933D4D70
A9E8C8DF24829B58404A5AF1B0D4C8668C35E3549E28204F2249BFC13B20C05AB0252C975E53F604F6
8C6E498C7B14ADB72DEBAC91221A8EB1AD581080144EB8900B4BF9D9792BE37EC6191AD183E2B60B80
174EECB66CA08C3AC07F51BA1C056130EC69
(2962866561507381037812023373119132136174928740191948464753572615608150431654289424
0699161014242748722092985192971233219332978756840330918906995731750173502760046230
9889329634915131558824154265990925147423039432179268635146251824722583191041856466
6812238445364105443256951780382932274957166301406575046967575195472147370079517748
5353964001227199625194468703595316973360848633495449100233980490435360003984197080
1709132747404324543063112301561331378099701557144397714665231171349871373169444260
8585230860620721238825486676442470637860896021951713092923229989700724358108486098
61946686929819844243978050289183932579134490)

              Tag: Private Exponent (0x420063), Type: Big Integer (0x04), Data:
42E22587E4C86D2227916855907F9FFC13B7872C228622725960BBFE286DF5407D12DE376744B8889F
64961C20747F911F6D7DBEA2B7A33E51776A7A239E60B5DE7F40F2451423F6BBDA638A497925675C41
519F0212D30E65422A21A0C6AD0993C1D7E1F0D8829AF6DFEBD94521CFB56CE1C5C4401D2915531CD8
04AC0A35EE57D2A43FFD7671AEAAD0AB090F17F8419073445AC6FB218BD3C7C5BEB9F3E7BF41E4E5F9
632D8492EB0CB2ADA41083E040535AE409AD866D1998A0335F253CDA2D21A95B2FEEBACEE64B969AAC
CAB322FA0ECBC75C3F0C15C267DBF431ABEDECAE191B72000B612E41E65EB93C9F08EEF67740B84BA3
```

```
2D9C5697ED91E1C8CCD1
(8443245174895379444005271604799260230892926003909979023717555224821060125754543376
7784572548361956988171698299646470720421482693177136888193036792745567241978525465
1563134111443535666762285503938943162690887352722584509971335262195690429465763025
0353012271016678109438436783045175140258175348964236928409393681548386835656355996
0083240144582861663067034612656838684532671451306824967975154417029908553292334726
4922418646157711740917740257893348537187310061748542914719908462677309906575874954
9012916144334864419540849289590925053239098897002962209075591476903506104513072002
7775807377133115061565847215462625944587473)

              Tag: Public Exponent (0x42006C), Type: Big Integer (0x04), Data:
0000000000010001 (65537)

              Tag: P (0x42005E), Type: Big Integer (0x04), Data:
0000000000000000F88C737435B8B3F5BDB2B2EB73DD5A665E2EE56C64E055169038F754ED3021D3E7
2AE82234DACD4A5FA12EDEB4874B70C5915BBA4571BEF55964389D8A4B8A79B628771BB4D634FBD18A
27AB5FB6973309C4AF9E27D269B1C4054B62012D1C52847E3679F71F91CF7FF6B646C9EDAAFE5B4684
5FC1190FA0EF80B8A45DE63973
(1745367882235574759531406606494904208317697766947574883552113610744546036919028555
8452306648039115584531058443187100231706098404487075147261583189304347929748761501
3179302290817326179061236123551945153992096043780673904683895898278957253623911965
2965661026100875930107579570187616835807709265506574501652347251)

              Tag: Q (0x420071), Type: Big Integer (0x04), Data:
0000000000000000F1BD952150D189707C316486F2054296802305055581B40ED503901BEF82CEC4E2A
0A564C58365E8C82B7D34A0305D407194B1D15C273015D1212969906267322827303B276D0C7585A21
EE6758A74E95BFECC5B544686325754E5D2602F0D5734C58F870AA2CA00E08122E940E4D6D0E11611D
47966482DF8845B8FF88D1FBB3
(1697559919409287473073270691819184555543786303570017161278829589177742257935213331
5937542177500233914129869978979171197443704590911425765232299081351275036342322736
0154199175459204889741734442211691523047572844058120222881886885491287288003162740
4576545896441724673089991030820894546678915947481233690463435699)

              Tag: Prime Exponent P (0x420060), Type: Big Integer (0x04), Data:
0000000000000000E9717156EAC62A305B15A63AC33E5A13DFCE0829C0AD7AFD904410F9B1350DF0AB
247F96F131B8B36C1245A562C5D833793CC77CB290DD1C2FF393C1540D1368B1905C1EA7C0B14EFB45
D9707A9B5273DB6EE2CB96F767D2511BEFEB82D34DD0AB24A821F1DBB2E5C3788347058DB696E43FDD
40DA6AA16534CE1F9E319B74C5
(1639293446803005458720969868260483904340869559892747980257973376806533511703524448
0628855202609208854391027532721039529768484690934852428621076516081600202446789835
5451710838289358616139513989793802462865701510274739483481278180610387030067996354
9119555347370391031048750367934579958058924517890530339727307973)

              Tag: Prime Exponent Q (0x420061), Type: Big Integer (0x04), Data:
0000000000000000EB6294819A364DC3AFCA507E6DCEDD65BA635F12331666842D6734E204B989671A
DC71E768C5980EED819D4525E858EA88A07133ACE15AE48B227A6D8A658A1A823707D49088FE727361
32C882B4767AAE2518E64633F6C69490B776B9CA53AD2F1C3ADD4976A66AC34521019D639ADAE5E550
2352B7900FA49B6F65B28DF4AD
(1652930233260360877164009581270876653302274732990784978406811898679958564595231733
9982579558341088652155019650557346701766522189975460026893723142306639992205151030
3506112061625550465141508486737215357000744823088101132230415333487053221792786168
4173027447633126604644165702439912791274674493378815733451846829)

              Tag: CRT Coefficient (0x420027), Type: Big Integer (0x04), Data:
0000000000000000CC75A52CAB58EB65878ACF7C19070C0A495D5376F40B86531B98B1E3B44E28D39D
B55898DB8AA317CE214814EFDD00C1D234D4C27168710A1A68CFDAE310F1A56E17E1A51F43D069137B
EEB7A6AEEF4DA2B3DFDE54D222E24C77209DC5C8C831B8F09F816D3EE628E76E93BAE2594229A59B36
EA1F507BE2DB99AE358896956E
(1435763798012376654831313191502672173012209873368433138518676814612157120707506466
7045770154196493466549555465061483043451957327963637081058313365314693719998991470
0546806962203378192554653895357894452540754748327409101333674007270138114124998378
2932644326982433007404666772284298917804379014569882316759799150)

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

	Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000800 (2048) 42007B01000006884200 7A01000000484200690100000020420 06A02000000040000000100000000042 006B020000000400000001000000004200920900000008000000004F9A557142000D02000000040000 0002000000000042000F01000000684200 5C0500000004000000080000000042009308000000 08F409F9 ADC43F836F42007F050000000400000000000000000042007C010000003042009407000000246662656 5 326136392D653336652D346463652D626238302D62363862353636386563376500000000 42000F0100 0005C042005C0500000004000000 0A000000004200930800000008396C4D8B5BDE066742007F050000 000400000000000000000042007C010000005884200570500000004000000040000000042009407000000 24666265653261363 92D653336652D346463652D626238302D6236386235363638656337650000000 0 42006401000005404200400100000538420042050000000400000000A00000000420045010000050042 004301000004F8420052040000010800000000000000000EAB4492BBB2364359408C57B8AF47003572C 81AAED719ED92D9B13C741CC196B717D1C98F0C250580E37AC3ADE11A7CD1AAEDE3A0424B53D332005 10CE7EEF71DED7E96E585D1D7BA3767A8DBFAD4D2701B5831A34552A827FC2CD398E659FD5063E1DFD 28A994B0E6A7449BBAD8DCF40E22943B841AA9E58519FA3575B4409ABFEB57F5723B45F7CE4E5277A2 D0ACCCBCD49608D6FF8A7C933D4D70A9E8C8DF24829B58404A5AF1B0D4C8668C35E3549E28204F2249 BFC13B20C05AB0252C975E53F604F68C6E498C7B14ADB72DEBAC91221A8EB1AD581080144EB8900B4B F9D9792BE37EC6191AD183E2B60B80174EECB66CA08C3AC07F51BA1C056130EC6942006304000001 00 42E22587E4C86D2227916855907F9FFC13B7872C228622725960BBFE286DF5407D12DE376744B8889F 64961C20747F911F6D7DBEA2B7A33E51776A7A239E60B5DE7F40F2451423F6BBDA638A497925675C41 519F0212D30E65422A21A0C6AD0993C1D7E1F0D8829AF6DFEBD94521CFB56CE1C5C4401D2915531CD8 04AC0A35EE57D2A43FFD7671AEAAD0AB090F17F8419073445AC6FB218BD3C7C5BEB9F3E7BF41E4E5F9 632D8492EB0CB2ADA41083E040535AE409AD866D1998A0335F253CDA2D21A95B2FEEBACEE64B969AAC CAB322FA0ECBC75C3F0C15C267DBF431ABEDECAE191B72000B612E41E65EB93C9F08EEF67740B84BA3 2D9C5697ED91E1C8CCD142006C04000000080000000000001000142005E04000000088000000000000000 00F88C737435B8B3F5BDB2B2EB73DD5A665E2EE56C64E055169038F754ED3021D3E72AE82234DACD4A 5FA12EDEB4874B70C5915BBA4571BEF55964389D8A4B8A79B628771BB4D634FBD18A27AB5FB6973309 C4AF9E27D269B1C4054B62012D1C52847E3679F71F91CF7FF6B646C9EDAAFE5B46845FC1190FA0EF80 B8A45DE63973420071040000008800000000000000000F1BD952150D189707C316486F2054296802305 05581B40ED503901BEF82CEC4E2A0A564C58365E8C82B7D34A0305D407194B1D15C273015D12129699 06267322827303B276D0C7585A21EE6758A74E95BFECC5B544686325754E5D2602F0D5734C58F870AA 2CA00E08122E940E4D6D0E11611D47966482DF8845B8FF88D1FBB34200600400000088000000000000 0 0000E9717156EAC62A305B15A63AC33E5A13DFCE0829C0AD7AFD904410F9B1350DF0AB247F96F131B8 B36C1245A562C5D833793CC77CB290DD1C2FF393C1540D1368B1905C1EA7C0B14EFB45D9707A9B5273 DB6EE2CB96F767D2511BEFEB82D34DD0AB24A821F1DBB2E5C3788347058DB696E43FDD40DA6AA16534 CE1F9E319B74C5420061040000008800000000000000000EB6294819A364DC3AFCA507E6DCEDD65BA63 5F12331666842D6734E204B989671ADC71E768C5980EED819D4525E858EA88A07133ACE15AE48B227A 6D8A658A1A823707D49088FE72736132C882B4767AAE2518E64633F6C69490B776B9CA53AD2F1C3ADD 4976A66AC34521019D639ADAE5E5502352B7900FA49B6F65B28DF4AD42002704000000880000000000 00 000000CC75A52CAB58EB65878ACF7C19070C0A495D5376F40B86531B98B1E3B44E28D39DB55898DB8A A317CE214814EFDD00C1D234D4C27168710A1A68CFDAE310F1A56E17E1A51F43D069137BEEB7A6AEEF 4DA2B3DFDE54D222E24C77209DC5C8C831B8F09F816D3EE628E76E93BAE2594229A59B36EA1F507BE2 DB99AE358896956E420028050000000400000004000000000 42002A02000000040000080000000000
5	Locate and Get (public key by name) In (header): batchOrderOption='TRUE' In: attributes={ Name={ Name='PublicKey1', NameType='00000001'}, objectType = '00000003' } 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: 
0x00000001 (1)
    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: Byte String (0x08), Data: 
5DF01D7748D64A16
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Maximum Items (0x42004F), Type: Integer (0x02), Data: 0x00000001 (1)
      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: Object 
Type
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 
0x00000003 (Public Key)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
7C7F588280A61C24
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x0000000B 
(Transparent RSA Public Key)



42007801000001484200770100000048420069010000002042006A020000000400000001000000042
006B0200000004000000010000000042001006000000080000000000000001420000D0200000004000 0
0002000000000420000F01000000B042005C0500000004000000080000000042009308000000085DF01D
7748D64A16420079010000008842004F020000000400000001000000004200080100000040420000A07
000000044E616D650000000042000B01000000284200550700000000A5075626C69634B657931000000
00000042005405000000040000000100000000420008010000002842000A070000000B4F626A656374
20547970650000000000042000B05000000040000000300000000042000F01000000384200 5C05000000
040000000A00000000420093080000000087C7F588280A61C244200790100000010420042050000000 04
```

```
0000000B00000000
```

Out: objectType = ‘00000003’, uuidRekeyedPublicKey, rekeyedPublicKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571
(Fri Apr 27 10:14:41 CEST 2012)
    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: Byte String (0x08), Data:
5DF01D7748D64A16
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000
(Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: d61b7a14-
6204-4272-bae5-1430dd2b6cba
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
7C7F588280A61C24
    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: 0x00000003
(Public Key)
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: d61b7a14-
6204-4272-bae5-1430dd2b6cba
      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:
```

```
0x0000000B (Transparent RSA Public Key)

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

            Tag: Key Material (0x420043), Type: Structure (0x01), Data:

              Tag: Modulus (0x420052), Type: Big Integer (0x04), Data:
0000000000000000EAB4492BBB2364359408C57B8AF47003572C81AAED719ED92D9B13C741CC196B71
7D1C98F0C250580E37AC3ADE11A7CD1AAEDE3A0424B53D33200510CE7EEF71DED7E96E585D1D7BA376
7A8DBFAD4D2701B5831A34552A827FC2CD398E659FD5063E1DFD28A994B0E6A7449BBAD8DCF40E2294
3B841AA9E58519FA3575B4409ABFEB57F5723B45F7CE4E5277A2D0ACCCBCD49608D6FF8A7C933D4D70
A9E8C8DF24829B58404A5AF1B0D4C8668C35E3549E28204F2249BFC13B20C05AB0252C975E53F604F6
8C6E498C7B14ADB72DEBAC91221A8EB1AD581080144EB8900B4BF9D9792BE37EC6191AD183E2B60B80
174EECB66CA08C3AC07F51BA1C056130EC69
(2962866561507381037812023373119132136174928740191948464753572615608150431654289424
0699161014242748722092985192971233219332978756840330918906995731750173502760046230
9889329634915131558824154265990925147423039432179268635146251824722583191041856466
6812238445364105443256951780382932274957166301406575046967575195472147370079517748
5353964001227199625194468703595316973360848633495449100233980490435360003984197080
1709132747404324543063112301561331378099701557144397714665231171349871373169444260
8585230860620721238825486676442470637860896021951713092923229989700724358108486098
6194668692981984424397805028918393257913449)

              Tag: Public Exponent (0x42006C), Type: Big Integer (0x04), Data:
0000000000010001 (65537)

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000800 (2048)



42007B01000002B042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A557142000D02000000040000
00020000000042000F010000006842005C05000000040000000800000000420093080000000085DF01D
7748D64A1642007F05000000040000000000000000042007C0100000030420094070000002464363162
376131342D363230342D343237322D626165352D31343330646432623663626100000000042000F0100
0001E842005C050000000400000000A000000004200930800000000087C7F588280A61C2442007F050000
00040000000000000000042007C01000001B042005705000000040000000300000000420094070000000
2464363162376131342D363230342D343237322D626165352D313433306464326236636261000000000
42006D0100000168420040010000016042004205000000040000000B0000000042004501000001284
200430100000120420052040000010800000000000000000EAB4492BBB2364359408C57B8AF47003572C
81AAED719ED92D9B13C741CC196B717D1C98F0C250580E37AC3ADE11A7CD1AAEDE3A0424B53D332005
10CE7EEF71DED7E96E585D1D7BA3767A8DBFAD4D2701B5831A34552A827FC2CD398E659FD5063E1DFD
28A994B0E6A7449BBAD8DCF40E22943B841AA9E58519FA3575B4409ABFEB57F5723B45F7CE4E5277A2
D0ACCCBCD49608D6FF8A7C933D4D70A9E8C8DF24829B58404A5AF1B0D4C8668C35E3549E28204F2249
BFC13B20C05AB0252C975E53F604F68C6E498C7B14ADB72DEBAC91221A8EB1AD581080144EB8900B4B
F9D9792BE37EC6191AD183E2B60B80174EECB66CA08C3AC07F51BA1C056130EC6942006C0400000008
0000000000010001420028050000000400000004000000000042002A020000000400000800000000000
```

6

Get Attributes

In: uuidRekeyedPrivateKey, attributeNames={'Link'}

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: 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: fbee2a69-
e36e-4dce-bb80-b68b5668ec7e

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

```
42007801000000A0420077010000003842006901000000204200 6A0200000004000000010000000042
```

Out: uuidRekeyedPrivateKey, attributes={ Link={LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidRekeyedPublicKey}, Link={LinkType='ReplacedObjectLink', LinkedObjectIdentifier=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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571
(Fri Apr 27 10:14:41 CEST 2012)

    Tag: 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: fbee2a69-
e36e-4dce-bb80-b68b5668ec7e

      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: d61b7a14-6204-4272-bae5-1430dd2b6cba

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

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

        Tag: Attribute Index (0x420009), Type: Integer (0x02), Data: 0x00000001
(1)

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

          Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000107
(Replaced Object Link)

          Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07),
Data: bbc58640-9ff2-4f8d-8a0f-8d977e1cc12c
```

```
42007B010000018042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A557142000D02000000040000
00010000000042000F010000012842005C0500000004000000000B000000042007F0500000004000000
000000000042007C010000010042009407000000246662656532613639 2D653336652D34646365 2D62
6238302D623638623536363865633765000000004200080100000058 42000A07000000044C696E6B00
000000042000B010000004042004B050000000400000102000000000 42004C07000000246436316237 61
31342D363230342D343237322D626165352D313433306464326236636261000000004200080100000 0
6842000A07000000044C696E6B0000000042000902000000040000000100000000 42000B0100000040
42004B05000000040000010700000000 42004C07000000246262633538363430 2D396666322D346638
642D386130662D3864393737653163633132630000000 0
```

7

Get Attributes

In: uuidRekeyedPublicKey, attributeNames={'Link'}

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

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

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

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

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

```
0x00000001 (1)

    Tag: 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: d61b7a14-
6204-4272-bae5-1430dd2b6cba

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

```
42007801000000A042007701000000384200690100000020042006A0200000004000000010000000042
006B020000000400000001000000042000D0200000004000000010000000042000F01000000584200
5C05000000040000000B000000004200790100000040420094070000002464363162376131342D3632
30342D343237322D626165352D313433306464326236636261000000000042000A07000000044C696E6B
00000000
```

Out: uuidRekeyedPublicKey, attributes={ Link={LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidRekeyedPrivateKey}, Link={LinkType='ReplacedObjectLink', 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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571
(Fri Apr 27 10:14:41 CEST 2012)

    Tag: 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: d61b7a14-
6204-4272-bae5-1430dd2b6cba
```

```
      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: fbee2a69-e36e-4dce-bb80-b68b5668ec7e

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

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

        Tag: Attribute Index (0x420009), Type: Integer (0x02), Data: 0x00000001
(1)

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

          Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000107
(Replaced Object Link)

          Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07),
Data: 9f5e2833-2df0-400d-9414-74ce8a4b9dee



42007B010000018042007A0100000048420069010000002042006A020000000400000001000000042
006B02000000040000000100000000420092090000000800000004F9A557142000D020000000040000
00010000000042000F010000012842005C0500000004000000B000000000042007F0500000004000000
000000000042007C010000010042009407000000246436316237613134 2D363230342D343237322D62
```

8

Get Attributes

In: uuidPrivateKey, attributeNames={'Link'}

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: 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: bbc58640-
9ff2-4f8d-8a0f-8d977e1cc12c
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
```

```
42007801000000A0420077010000003842006901000000204200 6A0200000004000000010000000042
006B02000000040000000100000000042000D020000000400000001000000042000F01000000584200
5C0500000004000000B00000000420079010000004042009407000000246262633538363430 2D3966
66322D346638642D386130662D3864393737653163633132630000000042000A07000000044C696E6B
00000000
```

Out: uuidPrivateKey, attributes={ Link={LinkType='PublicKeyLink', LinkedObjectIdentifier=uuidPublicKey}, Link={LinkType='ReplacementObjectLink', LinkedObjectIdentifier=uuidRekeyedPrivateKey} }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571
(Fri Apr 27 10:14:41 CEST 2012)
    Tag: 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: bbc58640-
9ff2-4f8d-8a0f-8d977e1cc12c
      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: 9f5e2833-2df0-400d-9414-74ce8a4b9dee

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

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

        Tag: Attribute Index (0x420009), Type: Integer (0x02), Data: 0x00000001 
(1)

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

          Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000106 
(Replacement Object Link)

          Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), 
Data: fbee2a69-e36e-4dce-bb80-b68b5668ec7e
```

```
42007B010000018042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A557142000D02000000040000
00010000000042000F010000012842005C05000000040000000B00000000042007F0500000004000000
000000000042007C0100000100420094070000002462626335383634302D396666322D346638642D38
6130662D38643937376531636331326300000000420008010000005842000A07000000044C696E6B00
000000420000B01000000040420004B050000000400000102000000000420004C0700000024396635653238
33332D326466302D343030642D393431342D37346365386134623964656500000000420008010000000
6842000A07000000044C696E6B00000000420009020000000400000001000000000420000B0100000040
42004B05000000040000010600000000042004C070000002466626565326136392D653336652D346463
652D626238302D62363862353636386563376500000000
```

9

Get Attributes

In: uuidPublicKey, attributeNames={'Link'}

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: 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: 9f5e2833-
2df0-400d-9414-74ce8a4b9dee
```

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

```
42007801000000A0420077010000003842006901000000204200 6A020000000400000001000000000 42
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000584200
5C05000000040000000B000000004200790100000040420094070000002439663565323833332D3264
66302D343030642D393431342D37346365386134623964656500000000042000A070000000044C696E6B
00000000
```

Out: uuidPublicKey, attributes={ Link={LinkType='PrivateKeyLink', LinkedObjectIdentifier=uuidPrivateKey}, Link={LinkType='ReplacementObjectLink', LinkedObjectIdentifier=uuidRekeyedPublicKey} }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571
(Fri Apr 27 10:14:41 CEST 2012)
    Tag: 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: 9f5e2833-
2df0-400d-9414-74ce8a4b9dee
      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: bbc58640-9ff2-4f8d-8a0f-8d977e1cc12c
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
```

	Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link Tag: Attribute Index (0x420009), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000106 (Replacement Object Link) Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07), Data: d61b7a14-6204-4272-bae5-1430dd2b6cba 42007B010000018042007A01000000484200690100000020042006A02000000040000000100000000042 006B0200000004000000010000000042009209000000080000000004F9A557142000D020000000400000 0001000000000042000F010000012842005C0500000004000000000B0000000042007F0500000004000000 000000000042007C0100000100420094070000002439663565323833332D326466302D343030642D39 3431342D373463653861346239646565000000000420008010000005842000A07000000044C696E6B00 00000042000B010000004042004B05000000040000010300000000042004C0700000024626263353836 34302D396666322D346638642D386130662D38643937376531636331326300000000420008010000000 6842000A07000000044C696E6B0000000042000902000000040000000100000000042000B0100000040 42004B0500000000400000106000000000042004C07000000246436316237613134 2D363230342D343237 322D626165352D3134333064643262366362610000000
10	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: 0x00000001 (1) Tag: 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: bbc58640-9ff2-4f8d-8a0f-8d977e1cc12c 42007801000000904200770100000038420069010000002042006A02000000040000000100000000042 006B02000000040000000100000000042000D02000000040000000100000000042000F0100000048420 0 5C05000000040000001400000000420079010000003042009407000000246262633538363430 2D3966 66322D346638642D386130662D38643937376531636331326300000000

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571 
(Fri Apr 27 10:14:41 CEST 2012)
    Tag: 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: bbc58640-
9ff2-4f8d-8a0f-8d977e1cc12c
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A557142000D020000000400000
0001000000042000F010000005842005C0500000004000000140000000042007F0500000004000000
00000000042007C010000003042009407000000246262633538363430 2D396666322D346638642D38
6130662D38643937376531636331326300000000
```

11 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: 
0x00000001 (1)

    Tag: 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: 9f5e2833-
2df0-400d-9414-74ce8a4b9dee



42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000001400000000420079010000003042009407000000243966356532383332D3264
66302D343030642D393431342D373463653861346239646565000000000
```

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: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571 
(Fri Apr 27 10:14:41 CEST 2012)

    Tag: 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: 9f5e2833-
2df0-400d-9414-74ce8a4b9dee



42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A557142000D02000000040000
```

	000100000000042000F01000000058420 05C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002439663565323833332D326466302D343030642D393431342D37346365386134623964656500000000
12	Destroy In: uuidRekeyedPrivateKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: fbee2a69-e36e-4dce-bb80-b68b5668ec7e 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B0200000004000000010000000042000D0200000004000000010000000042000F010000004842005C0500000004000000140000000042007901000000304200940700000024666265653261363932D653336652D346463652D626238302D62363862353636386563376500000000 Out: uuidRekeyedPrivateKey Tag: Response Message (0x42007B), Type: Structure (0x01), Data: Tag: Response Header (0x42007A), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:

	0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571 (Fri Apr 27 10:14:41 CEST 2012) Tag: 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: fbee2a69-e36e-4dce-bb80-b68b5668ec7e 42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420 06B0200000004000000010000000042009209000000080000000004F9A557142000D02000000040000 00010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000 0000000000042007C010000003042009407000000246662656532613639 2D653336652D346463652D62 6238302D623638623536363865633765000000000
13	Destroy In: uuidRekeyedPublicKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: d61b7a14-6204-4272-bae5-1430dd2b6cba 420078010000009042007701000000384200690100000002042006A02000000040000000100000000042 006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200 5C050000000400000014000000004200790100000030420094070000002464363162376131342D3632

```
30342D343237322D626165352D313433306464326236636261000000000
```

Out: uuidRekeyedPublicKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571
(Fri Apr 27 10:14:41 CEST 2012)
    Tag: 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: d61b7a14-
6204-4272-bae5-1430dd2b6cba
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000000400000001000000004200920900000008000000004F9A557142000D02000000040000
0001000000000042000F010000005842005C0500000004000000140000000042007F0500000004000000
0000000000042007C01000000304200940700000024643631623761313422D363230342D343237322D62
6165352D313433306464326236636261000000000
```

13.4 Test Case: Register Key Pair, Certify and Re-certify Public Key

Register a public/private key pair on the server. Request the server to have a certificate created using the Certify operation. Retrieve the certificate and its attributes, then execute the Re-certify operation to re-certify the public key. Finally, destroy all the objects.

This test case is aimed at exercising the functionality defined in the Basic Certificate Server Profile [KMIP-Spec]

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof].

Time	Request/Response messages

0	Register (Public Key)
	In: objectType='00000003', attributes={ CryptographicUsageMask='00000002' }, publicKey
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
	    Tag: 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: Public Key (0x42006D), Type: Structure (0x01), Data:
	        Tag: Key Block (0x420040), Type: Structure (0x01), Data:
	          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000003 (PKCS#1)
	          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
	            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 3082010A0282010100AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E440AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA

```
214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C7
95328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1
B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E5
4951662A6EDA29C6FC411335D5DC7426B0F6050203010001

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000800 (2048)
```

```
42007801000002104200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000001C84200
5C0500000004000000030000000042007901000001B04200570500000004000000030000000420091
01000000384200080100000030420000A07000000184372797074672617068696320557361676520
4D61736B42000B020000000400000002000000000042006D010000015842004001000001504200420500
0000040000000300000000420045010000011842004308000010E3082010A0282010100AB7F161C00
42496CCD6C6D4DADB91997343535777 6003ACF54B7AF1E440AFB80B64A8755F8002CFEBA6B184540A2
D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7EC114F3B176B7957C422E7D03FC6267FA2
A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA214900DF8B65089F98135B1C67B7
01675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C795328ABF70E1B42E7BB8B7F4E8AC
8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1B7AE64C54130FBC21D80E9C2CB06
C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E54951662A6EDA29C6FC411335D5DC
7426B0F605020301000100004200280500000000400000000400000000042002A020000000040000080000
000000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571
(Fri Apr 27 10:14:41 CEST 2012)

    Tag: 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: 3ddc1ae4-
```

	e212-46c7-a835-449fb94d12ff 42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042 006B0200000004000000010000000042009209000000080000000004F9A557142000D020000000040000 00010000000042000F01000000058420005C050000000400000003000000042007F050000000040000000 0000000000042007C0100000030420094070000002433646463316165342D653231322D343663372D61 3833352D343439666239346431326666600000000

1	Register (Private Key)
	
	In: objectType=’00000004’, attributes={ CryptographicUsageMask=‘00000001’, Link={ LinkType=‘PublicKeyLink’, LinkedObjectIdentifier=uuidPublicKey } }, privateKey
	
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
	    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003 (Register)
	    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
	      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000004 (Private Key)
	      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
	        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
	          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Cryptographic Usage Mask
	          Tag: Attribute Value (0x42000B), Type: Integer (0x02), Data: 0x00000001 (Sign)
	        Tag: 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: 3ddc1ae4-e212-46c7-a835-449fb94d12ff

```
      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:
0x00000003 (PKCS#1)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
308204A502010002820101000AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E44
0AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7
EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A411
00F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC829
5353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA8
09E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374
FE30E54951662A6EDA29C6FC411335D5DC7426B0F6050203010001028201003B12455D53C1816516C5
18493F6398AAFA72B17DFA894DB888A7D48C0A47F62579A4E644F86DA711FEC850CDD9DBBD17F69A44
3D2EC1DD60D3C618FA74CDE5FDAFABD6BAA26EB0A3ADB4DEF6480FB1218CD3B083E252E885B6F0729F
98B2144D2B72293E1B11D73393BC41F75B15EE3D7569B4995ED1A14425DA4319B7B26B0E8FEF17C375
42AE5C6D5849F87209567F3925A47B016D564859717BC57FCB4522D0AA49CE816E5BE7B3088193236E
C9EFFF140858045B73C5D79BAF38F7C67F04C5DCF0E3806AD982D1259058C3473E847179A878F2C6B3
BD968FB99EA46E9185892F3676E78965C2AED4877BA3917DF07C5E927474F19E764BA61DC38D63BF29
02818100D5C69C8C3CDC2464744A793713DAFB9F1DBC799FF96423FECD3CBA794286BCE920F4B5C183
F99EE9028DB6212C6277C4C8297FCFBCE7F7C24CA4C51FC7182FB8F4019FB1D5659674C5CBE6D5FA99
2051341760CD00735729A070A9E54D342BEBA8EF47EE82D3A01B04CEC4A00D4DDB41E35116FC221E85
4B43A696C0E6419B1B02818100CD5EA7702789064B673540CBFF09356AD80BC3D592812EBA47610B9F
AC6AECEFE22ACAE438459CDA74E59653D88C04189D34399BF5B14B920E34EF38A7D09FE69593396E8F
E735E6F0A6AE4990401041D8A406B6FD86A1161E45F95A3EAA5C1012E6662E44F15F335AC971E1766B
2BB9C985109974141B44D37E1E319820A55F02818100B2871237BF9FAD38C3316AB7877A6A868063E5
42A7186D431E8D27C19AC0414584033942E9FF6E2973BB7B2D8B0E94AD1EE82158108FBC8664517A5A
467FB963014BD5DCC2B4FB087C23039D11920DBE22FD9F16B4D89E23225CD455ADBAF32EF43F185864
A36D630309D6853F7714B39AAE1EBEE3938F87C2707E178C739F9F028181009690BED14B2AFAA26D98
6D592231EE27D71D49065BD2BA1F78157E20229881FD9D23227D0F8479EAEFA922FD75D5B16B1A561F
A6680B040CA0BDCE650B23B917A4B1BB7983A74FAD70E1C305CBEC2BFF1A85A726A1D90260E4F1084F
518234DCD3FE770B9520215BD543BB6A4117718754676A34171666A79F26E79C149C5AA102818100A0
C985A0A0A791A659F99731134C44F37B2E520A2CEA35800AD27241ED360DFDE6E8CA614F12047FD08B
76AC4D13C056A0699E2F98A1CAC91011294D71208F4ABAB33BA87AA0517F415BACA88D6BAC006088FA
601D349417E1F0C9B23AFFA4D496618DBC024986ED690BBB7B025768FF9DF8AC15416F489F8129C323
41A8B44F

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000800 (2048)



42007801000006104200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000005C84200
5C0500000004000000030000000042007901000005B04200570500000004000000040000000420091
01000000984200080100000030420000A070000000184372797074677261706869632055736167520
4D61736B42000B020000000400000001000000004200080100000058420000A07000000044C696E6B00
00000042000B0100000040420004B050000000400000102000000004200004C0700000024336464633161
65342D653231322D343663372D613833352D343439666239346431326666000000004200640100004
F842004001000004F04200420500000004000000030000000042004501000004B842004308000004A9
308204A502010002820101000AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E44
0AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7
EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A411
00F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC829
5353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA8
09E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374
FE30E54951662A6EDA29C6FC411335D5DC7426B0F6050203010001028201003B12455D53C1816516C5
18493F6398AAFA72B17DFA894DB888A7D48C0A47F62579A4E644F86DA711FEC850CDD9DBBD17F69A44
3D2EC1DD60D3C618FA74CDE5FDAFABD6BAA26EB0A3ADB4DEF6480FB1218CD3B083E252E885B6F0729F
```

```
98B2144D2B72293E1B11D73393BC41F75B15EE3D7569B4995ED1A14425DA4319B7B26B0E8FEF17C375
42AE5C6D5849F87209567F3925A47B016D564859717BC57FCB4522D0AA49CE816E5BE7B3088193236E
C9EFFF140858045B73C5D79BAF38F7C67F04C5DCF0E3806AD982D1259058C3473E847179A878F2C6B3
BD968FB99EA46E9185892F3676E78965C2AED4877BA3917DF07C5E927474F19E764BA61DC38D63BF29
02818100D5C69C8C3CDC2464744A793713DAFB9F1DBC799FF96423FECD3CBA794286BCE920F4B5C183
F99EE9028DB6212C6277C4C8297FCFBCE7F7C24CA4C51FC7182FB8F4019FB1D5659674C5CBE6D5FA99
2051341760CD00735729A070A9E54D342BEBA8EF47EE82D3A01B04CEC4A00D4DDB41E35116FC221E85
4B43A696C0E6419B1B02818100CD5EA7702789064B673540CBFF09356AD80BC3D592812EBA47610B9F
AC6AECEFE22ACAE438459CDA74E59653D88C04189D34399BF5B14B920E34EF38A7D09FE69593396E8F
E735E6F0A6AE4990401041D8A406B6FD86A1161E45F95A3EAA5C1012E6662E44F15F335AC971E1766B
2BB9C985109974141B44D37E1E319820A55F02818100B2871237BF9FAD38C3316AB7877A6A868063E5
42A7186D431E8D27C19AC0414584033942E9FF6E2973BB7B2D8B0E94AD1EE82158108FBC8664517A5A
467FB963014BD5DCC2B4FB087C23039D11920DBE22FD9F16B4D89E23225CD455ADBAF32EF43F185864
A36D630309D6853F7714B39AAE1EBEE3938F87C2707E178C739F9F028181009690BED14B2AFAA26D98
6D592231EE27D71D49065BD2BA1F78157E20229881FD9D23227D0F8479EAEFA922FD75D5B16B1A561F
A6680B040CA0BDCE650B23B917A4B1BB7983A74FAD70E1C305CBEC2BFF1A85A726A1D90260E4F1084F
518234DCD3FE770B9520215BD543BB6A4117718754676A34171666A79F26E79C149C5AA102818100A0
C985A0A0A791A659F99731134C44F37B2E520A2CEA35800AD27241ED360DFDE6E8CA614F12047FD08B
76AC4D13C056A0699E2F98A1CAC91011294D71208F4ABAB33BA87AA0517F415BACA88D6BAC006088FA
601D349417E1F0C9B23AFFA4D496618DBC024986ED690BBB7B025768FF9DF8AC15416F489F8129C323
41A8B44F000000000000004200280500000004000000040000000042002A0200000004000008000000
0000
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571
(Fri Apr 27 10:14:41 CEST 2012)

    Tag: 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: e3259cf3-
4cdc-4f60-8698-1789e2d83825
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
```

```
006B020000000400000001000000004200920900000008000000004F9A557142000D02000000040000
0001000000042000F01000000584200 5C0500000004000000030000000042007F0500000004000000
000000000042007C01000000304200940700000024653332353963663332D346364632D346636302D38
3639382D313738396532643833383235000000000
```

2

Add attribute

In: uuidPublicKey, attribute={ 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:
0x00000001 (1)

    Tag: 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: 3ddc1ae4-
e212-46c7-a835-449fb94d12ff

      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: e3259cf3-4cdc-4f60-8698-1789e2d83825
```

```
42007801000000F04200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000A84200
5C0500000004000000D00000000420079010000009042009407000000243364646331616534 2D6532
31322D343663372D613833352D343439666239346431326666000000004200080100000058420000A07
000000044C696E6B000000000042000B010000004042004B050000000400000103000000000042004C0700
000024653332353963663332D346364632D346636302D383639382D313738396532643833383235000
0000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571 
(Fri Apr 27 10:14:41 CEST 2012)
    Tag: 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: 3ddc1ae4-
e212-46c7-a835-449fb94d12ff
      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: e3259cf3-4cdc-4f60-8698-1789e2d83825
```

```
42007B010000011042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A557142000D020000000040000
0001000000000042000F01000000B842005C05000000040000000D000000042007F050000000400000000
00000000042007C0100000090420094070000002433646463316165342D653231322D343663372D61
3833352D343439666239346431326666000000004200080100000058420000A070000000044C696E6B00
000000042000B010000004042004B05000000040000010300000000042004C0700000024653332353963
66332D346364632D346636302D383639382D31373839653264383338323500000000
```

3 Certify

In: uuidPublicKey, certificateSigningRequest, attributes={ CryptographicUsageMask='00000003', Name={ NameValue='CertifiedCertificate', 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: 
0x00000001 (1)

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

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

    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000006 
(Certify)

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 3ddc1ae4-
e212-46c7-a835-449fb94d12ff

      Tag: Certificate Request Type (0x420019), Type: Enumeration (0x05), Data: 
0x00000002 (PKCS#10)

      Tag: Certificate Request (0x420018), Type: Byte String (0x08), Data: 
3082028130820169020100303C310B3009060355040613025553310D300B060355040A130441434D45
310D300B060355040B13044B4D4950310F300D06035504031306436C69656E7430820122300D06092A
864886F70D01010105000382010F003082010A0282010100AB7F161C0042496CCD6C6D4DADB9199734
35357776003ACF54B7AF1E440AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D718
12B205387C0F6583BC4D7DC7EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833
E5A5F4BB0B1434F4E795A41100F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A
7F081FCEC80B64E8A0ECC8295353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA
7D0CA34142CB76F91F013DA809E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C28
15C3612A29A82D73A1F99374FE30E54951662A6EDA29C6FC411335D5DC7426B0F6050203010001A000
300D06092A864886F70D010105050003820101002D90F5492C3DF1771DF4E87E1087CB952197319A96
96E2D588EFDA580D8D3304427B997CD921AD7C674AEA413FBA85FD61E6A481DE9AB2E8A4FF43C02655
015D3437F783FE0C781519CD08FFD3C007C7FADE9632FE5659E2CAC35BD6AAF3E13DC18097D996DF01
B66FC5E26CA109380863A209125CC0FD79533F327FA1CAD444D89D3FF81B92A91428C469C846090FD1
324846E12D01671962C332A7826152DAAF486CC867185C2E27CAF2F009898DB07FE4B45C518192AA49
3D8F8C0198DB67F90672AB6DE05A08032941377F473D80716D85ADC6182003AB34942302214EB3895F
15403F2616ADFD6BB5E6AA47FA38C9DFC73F4DE80DDB91BDB04D21C82BA6

      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: 0x00000003 
(Sign, Verify)

        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:
CertifiedCertificate

            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001
(Uninterpreted Text String)
```

```
42007801000003C042007701000000384200690100000020420006A02000000004000000010000000042
006B02000000004000000010000000042000D0200000000400000001000000042000F01000003784200
5C05000000004000000006000000004200790100000360420094070000002433646463316165342D6532
31322D343663372D613833352D34343966623934643132666600000000420019050000000400000002
00000000420018080000028530820281308201690201003 03C310B30090603550406130255533 10D30
0B060355040A130441434D45310D300B060355040B13044B4D4950310F300D06035504031306436C69
656E7430820122300D06092A864886F70D01010105000382010F003082010A0282010100AB7F161C00
42496CCD6C6D4DADB919973435357776003ACF54B7AF1E440AFB80B64A8755F8002CFEBA6B184540A2
D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7EC114F3B176B7957C422E7D03FC6267FA2
A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA214900DF8B65089F98135B1C67B7
01675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C795328ABF70E1B42E7BB8B7F4E8AC
8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1B7AE64C54130FBC21D80E9C2CB06
C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E54951662A6EDA29C6FC411335D5DC
7426B0F6050203010001A000300D06092A864886F70D010105050003820101002D90F5492C3DF1771D
F4E87E1087CB952197319A9696E2D588EFDA580D8D3304427B997CD921AD7C674AEA413FBA85FD61E6
A481DE9AB2E8A4FF43C02655015D3437F783FE0C781519CD08FFD3C007C7FADE9632FE5659E2CAC35B
D6AAF3E13DC18097D996DF01B66FC5E26CA109380863A209125CC0FD79533F327FA1CAD444D89D3FF8
1B92A91428C469C846090FD1324846E12D01671962C332A7826152DAAF486CC867185C2E27CAF2F009
898DB07FE4B45C518192AA493D8F8C0198DB67F90672AB6DE05A08032941377F473D80716D85ADC618
2003AB34942302214EB3895F15403F2616ADFD6BB5E6AA47FA38C9DFC73F4DE80DDB91BDB04D21C82B
A60000004200910100000088420008010000003042000A070000001843727970746F67726170686963
20557361676520 4D61736B42000B02000000004000000030000000042000801000000484200 0A070000
00044E616D650000000042000B010000003042005507000000144365727469666965644365727466966
6963617465000000004200540500000000400000001000000000
```

Out: uuidCertificate

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571
(Fri Apr 27 10:14:41 CEST 2012)

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

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

    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000006
```

	(Certify) Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 25fc6fbe-d7d3-4c8e-83ad-1879fa5990fa 42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042 006B02000000040000000100000000420092090000000800000004F9A557142000D020000000400000 0001000000000042000F010000005842005C050000000400000006000000000042007F0500000004000000 000000000042007C010000003042009407000000243235666336666652D643764332D346338652D38 3361642D31383739666135393930666100000000
4	Get (certificate) In: uuidCertificate Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: 25fc6fbe-d7d3-4c8e-83ad-1879fa5990fa 42007801000000904200770100000038420069010000002042006A02000000040000000100000000042 006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200 5C05000000040000000A000000004200790100000030420094070000002432356663366662652D6437 64332D346338652D383361642D31383739666135393930666100000000 Out: certificate

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5571
(Fri Apr 27 10:14:41 CEST 2012)

    Tag: 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: 0x00000001
(Certificate)

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 25fc6fbe-
d7d3-4c8e-83ad-1879fa5990fa

      Tag: Certificate (0x420013), Type: Structure (0x01), Data:

        Tag: Certificate Type (0x42001D), Type: Enumeration (0x05), Data:
0x00000001 (X.509)

        Tag: Certificate Value (0x42001E), Type: Byte String (0x08), Data:
308203263082020EA00302010202146D0C0F4F2FEFEAF0D23D3BA25D2F70F5EA4AEFCB300D06092A86
4886F70D01010505003003B310B3009060355040613025553310D300B060355040A130454455354310E
300C060355040B13054F41534953310D300B060355040313044B4D4950301E170D3132303432373130
313434315A170D3133303432373130313434315A303C310B3009060355040613025553310D300B0603
55040A130441434D45310D300B060355040B13044B4D4950310F300D060355040313064366C69656E74
30820122300D06092A864886F70D01010105000382010F003082010A0282010100AB7F161C0042496C
CD6C6D4DADB919973435357776003ACF54B7AF1E440AFB80B64A8755F8002CFEBA6B184540A2D66086
D74648346D75B8D71812B205387C0F6583BC4D7DC7EC114F3B176B7957C422E7D03FC6267FA2A6F89B
9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA214900DF8B65089F98135B1C67B701675A
BDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C795328ABF70E1B42E7BB8B7F4E8AC8C810C
DB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7
CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E54951662A6EDA29C6FC411335D5DC7426B0
F605020301001A321301F301D0603551D0E0416041404E57BD2C431B2E816E180A19823FAC858273F
6B300D06092A864886F70D01010505000382010100051E9CC2F0900CD9C71E7DD3E407933CACCA299E6
C41FA02516386E928F506B04062CCE90444EDEC933CABA74B990AB0847C7B73278D388A349F99F296B
F458EC2C2C163E8D87BBEE47D233B9149661DD9A4C0AE559252A5DE1DFEB69CFB77138CBE0BB45B911
FC0EF675C37B749275545836E33CF738782397AF4BC3707AC14ABA5724E083BDB0D28FD2747CDD8BCA
74CE925692F4D06C0D2B74D8D2B540B7A1083189E5E0F49F0B740654D7D9F3FAA9B4C0F9056FE4F52E
4BEE812FE486194CCD478D65957BA63FBCB0C31F870283AB4E849C20993D6BECB0F27055B103AF3B66
75D123CD3B7179A46C77C73AE00FFDEFA9B125DA071EAD10D85EAD0D0D441F



42007B010000041042007A0100000048420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042009209000000080000000004F9A557142000D0200000004000000
00010000000042000F01000003B842005C05000000040000000A000000042007F0500000004000000
00000000042007C010000039042005705000000040000000100000000420094070000002432356663
```

```
366662652D643764332D346338652D383361642D313837396661353939306661000000004200130100
00034842001D0500000004000000010000000042001E080000032A308203263082020EA00302010202
146D0C0F4F2FEFEAF0D23D3BA25D2F70F5EA4AEFCB300D06092A864886F70D0101050500303B310B30
0906035504061302555331 0D300B060355040A13045445535431 0E300C060355040B13054F41534953
310D300B060355040313044B4D4950301E170D3132303432373130313434315A170D31333034323731
30313434315A303C310B3009060355040613025553310D300B060355040A130441434D45310D300B06
0355040B13044B4D4950310F300D06035504031306436C69656E7430820122300D06092A864886F70D
01010105000382010F003082010A0282010100AB7F161C0042496CCD6C6D4DADB919973435357776 00
3ACF54B7AF1E440AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C
0F6583BC4D7DC7EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B
1434F4E795A41100F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC8
0B64E8A0ECC8295353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142
CB76F91F013DA809E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29
A82D73A1F99374FE30E54951662A6EDA29C6FC411335D5DC7426B0F6050203010001A321301F301D06
03551D0E0416041404E57BD2C431B2E816E180A19823FAC858273F6B300D06092A864886F70D010105
050003820101 0051E9CC2F0900CD9C71E7DD3E407933CACCA299E6C41FA02516386E928F506B04062C
CE90444EDEC933CABA74B990AB0847C7B73278D388A349F99F296BF458EC2C2C163E8D87BBEE47D233
B9149661DD9A4C0AE559252A5DE1DFEB69CFB77138CBE0BB45B911FC0EF675C37B749275545836E33C
F738782397AF4BC3707AC14ABA5724E083BDB0D28FD2747CDD8BCA74CE925692F4D06C0D2B74D8D2B5
40B7A1083189E5E0F49F0B740654D7D9F3FAA9B4C0F9056FE4F52E4BEE812FE486194CCD478D65957B
A63FBCB0C31F870283AB4E849C20993D6BECB0F27055B103AF3B6675D123CD3B7179A46C77C73AE00F
FDEFA9B125DA071EAD10D85EAD0D0D441F000000000000
```

5

Get Attribute List

In: uuidCertificate

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: 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: 25fc6fbe-
d7d3-4c8e-83ad-1879fa5990fa
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000 42000D0200000004000000010000000042000F01000000484200
5C05000000040000000C000000004200790100000030420094070000002432356663366662652D6437
64332D346338652D383361642D313837396661353939306661 00000000
```

Out: uuidCertificate, attributeNames={ * }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572
(Fri Apr 27 10:14:42 CEST 2012)
    Tag: 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: 25fc6fbe-
d7d3-4c8e-83ad-1879fa5990fa
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data:
Cryptographic Length
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate
Length
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: X.509
Certificate Identifier
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: X.509
Certificate Issuer
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: X.509
Certificate Subject
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digital
Signature Algorithm
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate
Issuer
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate
Type
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate
```

	Subject Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate Identifier 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: Link Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Lease Time 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: Last Change Date 42007B01000002E042007A0100000048420069010000002042006A02000000040000000100000000042 006B02000000040000000100000000420092090000000800000004F9A557242000D02000000040000 0001000000000042000F01000002884205C0500000004000000C000000000042007F0500000004000000 000000000042007C01000002604200940700000024323566633666626 52D643764332D346338652D38 3361642D31383739666135393930666100000000042000A070000001443727970746F67726170686963 204C656E677468000000000042000A07000000124365727469666963617465204C656E67746800000000 000042000A070000001C582E3530392043657274696669636174652049646E746966696572000000 0042000A070000001858 2E353039204365727469666963617465204973737565724 2000A0700000019 582E3530392043657274696669636174652053756 26A6563740000000000000042000A070000001B44 69676974616C205369676E617475726520416C676F726974686D0000000000042000A07000000124365 72746966696361746520497373756572000000000000042000A070000001043657274696669636174 65 205479706542000A07000000134365727469666963617465205375626A65637400000000000042000A07 0000001643657274696669636174652049646E746966696572000042000A07000000055374617465 00000042000A07000000064469676573740000420 00A07000000044C696E6B000000000 42000A070000 000A4C65617365205469 6D650000000000000042000A070000000C496E697469616C204461746500000 0 0042000A07000000011556E697175652049646E746966696572000000000000000042000A0700000004 4E616D65000000000042000A0700000018437279707 46F6772617068696320557361676520 4D61736B42 000A070000000B4F626A6563742054797065000000000000042000A07000000104C6173742043686 16E67 652044617465
6	Get Attributes In: uuidCertificate, attributeNames={'Certificate Identifier', 'Certificate Issuer', 'Certificate Subject', 'Certificate Type'} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data:

```
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: 25fc6fbe-
d7d3-4c8e-83ad-1879fa5990fa
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate 
Identifier
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate 
Issuer
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate 
Subject
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Certificate 
Type
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digital 
Signature Algorithm
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: 
Cryptographic Length
```

```
4200780100000150420077010000003842006901000000204200 6A02000000040000000100000000042
```

Out: uuidCertificate, 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: 
0x00000001 (1)

  Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572 
(Fri Apr 27 10:14:42 CEST 2012)

  Tag: 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: 25fc6fbe-
d7d3-4c8e-83ad-1879fa5990fa

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

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

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

     Tag: Issuer (0x42003B), Type: Text String (0x07), Data: 
CN=KMIP,OU=OASIS,O=TEST,C=US

     Tag: Serial Number (0x420087), Type: Text String (0x07), Data: 
622548936592496278691702430160544827296587640779

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

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

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

     Tag: Certificate Issuer Distinguished Name (0x420017), Type: Text String 
(0x07), Data: CN=KMIP,OU=OASIS,O=TEST,C=US

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

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

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

     Tag: Certificate Subject Distinguished Name (0x42001C), Type: Text 
String (0x07), Data: CN=Client,OU=KMIP,O=ACME,C=US

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

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

    Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 
0x00000001 (X.509)

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

    Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digital 
Signature Algorithm
```

```
        Tag: Attribute Value (0x42000B), Type: Enumeration (0x05), Data: 
0x00000003 (SHA-1 with RSA Encryption (PKCS#1 v1.5))

      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: 0x00000800 
(2048)
```

42007B010000029842007A0100000048420069010000002042006A02000000040000000100000000420
06B02000000040000000100000000420092090000000800000004F9A557242000D020000000400000
00010000000042000F010000024042005C0500000004000000B000000042007F0500000004000000
000000000042007C01000002184200940700000024323566336662652D643764332D346338652D38
3361642D31383739666135393930666100000000420008010000008842000A07000000164365727469
666963617465204964656E746966696572000042000B010000006042003B070000001C434E3D4B4D49
502C4F553D4F415349532C4F3D544553542C433D555300000000420087070000003036323235343839
3336353932343936323738363931373032343330313630353434383237323936353837363430373739
420008010000005042000A07000000124365727469666963617465204973737565720000000000042
000B0100000028420017070000001C434E3D4B4D49502C4F553D4F415349532C4F3D544553542C433D
555300000000420008010000005042000A07000000134365727469666963617465205375626A656374
000000000042000B010000002842001C070000001D434E3D436C69656E742C4F553D4B4D49502C4F3D
41434D452C433D5553000000420008010000002842000A070000001043657274696669636174652054
79706542000B05000000040000000100000000420008010000003842000A070000001B446967697461
6C205369676E617475726520416C676F726974686D000000000042000B0500000004000000030000000
00420008010000003042000A070000001443727970746F67726170686963204C656E677468000000000
42000B02000000040000080000000000

7

Re-certify

In: uuidCertificate, certificateSigningRequest, attributes={ CryptographicUsageMask='00000003', Name={ NameValue='RecertifiedCertificate', 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: 
0x00000001 (1)

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

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

    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000007 (Re-
certify)

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 25fc6fbe-
```

```
d7d3-4c8e-83ad-1879fa5990fa

      Tag: Certificate Request Type (0x420019), Type: Enumeration (0x05), Data: 
0x00000002 (PKCS#10)

      Tag: Certificate Request (0x420018), Type: Byte String (0x08), Data: 
3082028130820169020100303C310B30090603550406130255533110D300B060355040A130441434D45
310D300B060355040B13044B4D4950310F300D06035504031306436C69656E7430820122300D06092A
864886F70D01010105000382010F003082010A0282010100AB7F161C0042496CCD6C6D4DADB9199734
35357776003ACF54B7AF1E440AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D718
12B205387C0F6583BC4D7DC7EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833
E5A5F4BB0B1434F4E795A41100F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A
7F081FCEC80B64E8A0ECC8295353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA
7D0CA34142CB76F91F013DA809E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C28
15C3612A29A82D73A1F99374FE30E54951662A6EDA29C6FC411335D5DC7426B0F6050203010001A000
300D06092A864886F70D01010505000382010100 2D90F5492C3DF1771DF4E87E1087CB952197319A96
96E2D588EFDA580D8D3304427B997CD921AD7C674AEA413FBA85FD61E6A481DE9AB2E8A4FF43C02655
015D3437F783FE0C781519CD08FFD3C007C7FADE9632FE5659E2CAC35BD6AAF3E13DC18097D996DF01
B66FC5E26CA109380863A209125CC0FD79533F327FA1CAD444D89D3FF81B92A91428C469C846090FD1
324846E12D01671962C332A7826152DAAF486CC867185C2E27CAF2F009898DB07FE4B45C518192AA49
3D8F8C0198DB67F90672AB6DE05A08032941377F473D80716D85ADC6182003AB34942302214EB3895F
15403F2616ADFD6BB5E6AA47FA38C9DFC73F4DE80DDB91BDB04D21C82BA6

      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: 0x00000003 
(Sign, Verify)

        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: 
RecertifiedCertificate

            Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001 
(Uninterpreted Text String)



42007801000003C042007701000000384200690100000020042006A020000000400000001000000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000003784200
5C0500000004000000070000000042007901000003604200940700000024323566336666652D6437
64332D346338652D383361642D31383739666135393930666100000000420019050000000400000002
0000000042001808000002853082028130820169020100303C310B30090603550406130255533110D30
0B060355040A130441434D45310D300B060355040B13044B4D4950310F300D06035504031306436C69
656E7430820122300D06092A864886F70D01010105000382010F003082010A0282010100AB7F161C00
42496CCD6C6D4DADB919973435357776003ACF54B7AF1E440AFB80B64A8755F8002CFEBA6B184540A2
D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7EC114F3B176B7957C422E7D03FC6267FA2
A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA214900DF8B65089F98135B1C67B7
01675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C795328ABF70E1B42E7BB8B7F4E8AC
8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1B7AE64C54130FBC21D80E9C2CB06
C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E54951662A6EDA29C6FC411335D5DC
7426B0F6050203010001A000300D06092A864886F70D01010505000382010100 2D90F5492C3DF1771D
F4E87E1087CB952197319A9696E2D588EFDA580D8D3304427B997CD921AD7C674AEA413FBA85FD61E6
A481DE9AB2E8A4FF43C02655015D3437F783FE0C781519CD08FFD3C007C7FADE9632FE5659E2CAC35B
D6AAF3E13DC18097D996DF01B66FC5E26CA109380863A209125CC0FD79533F327FA1CAD444D89D3FF8
1B92A91428C469C846090FD1324846E12D01671962C332A7826152DAAF486CC867185C2E27CAF2F009
898DB07FE4B45C518192AA493D8F8C0198DB67F90672AB6DE05A08032941377F473D80716D85ADC618
2003AB34942302214EB3895F15403F2616ADFD6BB5E6AA47FA38C9DFC73F4DE80DDB91BDB04D21C82B
```

	A6000000420091010000008842000801000000304200 0A07000000184372797074 6F67726170686963
	20557361676520 4D61736B42000B0200000004000000030000000042000801000000484200 0A070000
	00044E616D650000000042000B01000000304200550700000016526563657274696669656443657274
	696669636174650000420054050000000400000001000000000
	
	Out: uuidRecertifiedCertificate
	
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
	    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572 (Fri Apr 27 10:14:42 CEST 2012)
	    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
	  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
	    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000007 (Re-certify)
	    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
	    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
	      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1d4786cd-9d9a-41cb-90f7-bc0471c69779
	
	42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000 42
	006B02000000040000000100000000420092090000000800000004F9A557242000D0200000004 0000
	00010000000042000F01000000584200 5C0500000004000000070000000042007F050000000 4000000
	000000000042007C010000003042009407000000243164343738366364 2D396439612D343163622D39
	3066372D626330343731633639373739 00000000

8	Get Attributes In: uuidPrivateKey, attributeNames={'Link'} Tag: Request Message (0x420078), Type: Structure (0x01), Data:

```
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: e3259cf3-
4cdc-4f60-8698-1789e2d83825
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
```

```
42007801000000A04200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000584200
5C05000000040000000B00000000420079010000004042009407000000246533323539636633 2D3463
64632D346636302D383639382D3137383965326438333832350000000042000A07000000044C696E6B
00000000
```

Out: uuidPrivateKey, attributes={ 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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572 
(Fri Apr 27 10:14:42 CEST 2012)
    Tag: 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: e3259cf3-
4cdc-4f60-8698-1789e2d83825
      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: 3ddc1ae4-e212-46c7-a835-449fb94d12ff


42007B010000011042007A0100000048420069010000002042006A020000000400000001000000042
006B02000000040000000100000000420092090000000800000004F9A557242000D020000000040000
00010000000042000F01000000B842005C050000000400000000B000000042007F050000000400000000
000000000042007C010000009042009407000000246533323539636332D346364632D346636302D38
3639382D313738396532643833383235000000004200080100000058420000A07000000044C696E6B00
000000042000B010000004042004B05000000040000010200000000042004C0700000024336464633161
65342D653231322D343663372D613833352D343439666239346431326666600000000
```

9

Get Attributes

In: uuidPublicKey, attributeNames={'Link'}

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: 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: 3ddc1ae4-
e212-46c7-a835-449fb94d12ff
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
```

```
42007801000000A04200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000584200
5C0500000004000000000B0000000042007901000000404200940700000024336464633161653424D6532
31322D343663372D613833352D3434396662393464313266660000000042000A07000000044C696E6B
00000000
```

Out: uuidPublicKey, attributes={ Link={LinkType=‘PrivateKeyLink’, LinkedObjectIdentifier=uuidPrivateKey}, Link={LinkType=‘CertificateLink’, LinkedObjectIdentifier=uuidRecertifiedCertificate} }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572
(Fri Apr 27 10:14:42 CEST 2012)
    Tag: 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: 3ddc1ae4-
e212-46c7-a835-449fb94d12ff
      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: e3259cf3-4cdc-4f60-8698-1789e2d83825
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
        Tag: Attribute Index (0x420009), Type: Integer (0x02), Data: 0x00000001
(1)
```

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

          Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000101
(Certificate Link)

          Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07),
Data: 1d4786cd-9d9a-41cb-90f7-bc0471c69779
```

```
42007B010000018042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A557242000D020000000400000
0001000000000042000F010000012842005C05000000040000000B0000000042007F0500000004000000
000000000042007C0100000100420094070000002433646463316165342D653231322D343663372D61
3833352D34343966623934643132666600000000420008010000005842000A07000000044C696E6B00
00000042000B01000000404042004B05000000040000010300000000042004C070000002465333235396 3
66332D346364632D346636302D383639382D3137383965326438333832350000000042000801000000
6842000A07000000044C696E6B00000000420009020000000400000001000000000042000B0100000040
42004B050000000400000101000000000042004C07000000243164343738366364 2D396439612D343163
622D393066372D626330343731633639373739 00000000
```

10

Get Attributes

In: uuidCertificate, attributeNames={'Link'}

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: 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: 25fc6fbe-
d7d3-4c8e-83ad-1879fa5990fa

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

```
42007801000000A042007701000000384200690100000020420006A0200000004000000010000000042
006B02000000040000000100000000042000D020000000400000001000000000042000F010000005842000
5C05000000040000000B00000000420079010000004042009407000000243235666336666262652D6437
64332D346338652D383361642D3138373966613539393066610000000042000A07000000044C696E6B
00000000
```

Out: uuidCertificate, attributes={ Link={LinkType=‘PublicKeyLink’, LinkedObjectIdentifier=uuidPublicKey},

Link={LinkType='ReplacementObjectLink', LinkedObjectIdentifier=uuidRecertifiedCert }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572
(Fri Apr 27 10:14:42 CEST 2012)
    Tag: 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: 25fc6fbe-
d7d3-4c8e-83ad-1879fa5990fa
      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: 3ddc1ae4-e212-46c7-a835-449fb94d12ff
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
        Tag: Attribute Index (0x420009), Type: Integer (0x02), Data: 0x00000001
(1)
        Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
          Tag: Link Type (0x42004B), Type: Enumeration (0x05), Data: 0x00000106
(Replacement Object Link)
```

```
          Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07),
Data: 1d4786cd-9d9a-41cb-90f7-bc0471c69779
```

```
42007B010000018042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A557242000D020000000400000
00010000000042000F010000012842005C0500000004000000B000000042007F050000000400000000
0000000042007C010000010042009407000000243235666336666262652D643764332D346338652D38
3361642D3138373966613539393066610000000042000801000000584200A07000000044C696E6B00
00000042000B01000000404200 4B0500000004000000102000000042004C070000002433646463316165342D653231322D343663372D613833352D3434396662393464313266660000000042000801000000
6842000A070000000044C696E6B000000004200090200000004000000010000000042000B0100000040
42004B05000000040000010600000000042004C070000002431643437383663642D396439612D343163
622D393066372D62633034373163363937373900000000
```

11

Get Attributes

In: uuidRecertifiedCertificate, attributeNames={'Link', 'Certificate Identifier', '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:
0x00000001 (1)

    Tag: 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: 1d4786cd-
9d9a-41cb-90f7-bc0471c69779

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

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

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

```
42007801000000D0420077010000003842006901000000020420006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F010000008842000
5C0500000004000000B00000000420079010000007042009407000000243164343738366364 2D3964
39612D343163622D393066372D626330343731633639373739000000000042000A07000000044C696E6B
0000000042000A07000000164365727469666963617465204964656E746966696572000042000A0700
0000044E616D6500000000
```

Out: uuidRecertifiedCertificate, attributes={ Link={LinkType=‘PublicKeyLink’, LinkedObjectIdentifier=uuidPublicKey}, Link={LinkType=‘ReplacedObjectLink’, LinkedObjectIdentifier=uuidCertificate}, CertificateIdentifier={*}, Name={NameValue='CertifiedCertificate', NameType='00000001'}, Name={NameValue='RecertifiedCertificate', NameType='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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572
(Fri Apr 27 10:14:42 CEST 2012)
    Tag: 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: 1d4786cd-
9d9a-41cb-90f7-bc0471c69779
      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: 0x00000107
(Replaced Object Link)
          Tag: Linked Object Identifier (0x42004C), Type: Text String (0x07),
Data: 25fc6fbe-d7d3-4c8e-83ad-1879fa5990fa
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Link
        Tag: Attribute Index (0x420009), Type: Integer (0x02), Data: 0x00000001
(1)
        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: 3ddc1ae4-e212-46c7-a835-449fb94d12ff

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

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

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

          Tag: Issuer (0x42003B), Type: Text String (0x07), Data:
CN=KMIP,OU=OASIS,O=TEST,C=US

          Tag: Serial Number (0x420087), Type: Text String (0x07), Data:
202841986457594585657309264944215936885082481100

      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:
CertifiedCertificate

          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 Index (0x420009), Type: Integer (0x02), Data: 0x00000001
(1)

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

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

          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001
(Uninterpreted Text String)
```

```
42007B01000002C042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A557242000D02000000040000
0001000000000042000F010000026842005C05000000040000000B000000000042007F0500000004000000
000000000042007C01000002404200940700000024316434373836636 42D396439612D343163622D39
3066372D626330343731633639373739000000004200080100000005842000A07000000044C696E6B00
000000042000B01000000404200 4B05000000040000010700000000042004C07000000243235666336 66
62652D643764332D346338652D383361642D313837396661353939306661000000004200080 1000000
6842000A07000000044C696E6B000000004200090200000004000000010000000042000B0100000040
42004B0500000000400000102000000000420 04C070000002433646463316165342D653231322D343663
372D613833352D3434396662393464313266660000000042000801000000088 42000A07000000164365
72746966696361746520496 4656E74696669657200004 2000B01000000604200 3B070000001C434E3D
4B4D49502C4F553D4F415349532C4F3D544553542C433D555300000000420087070000003032303238
343139383634353735393435383536353733303932363439343432313539333638383530383234 3831
31303042000801000000484 2000A07000000044E616D6500000000420 00B010000003042005507 0000
0014436572746966696564436572746966696361746500000000420054050000000400000001000000
004200080100000058420 00A07000000044E616D650000000042000902000000040000000100000000
42000B01000000304200550700000016526563657274696669656443657274696669636174650000 42
00540500000004000000010000 0000
```

12

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: 
0x00000001 (1)
    Tag: 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: e3259cf3-
4cdc-4f60-8698-1789e2d83825
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C0500000004000000140000000042007901000000304200940700000024653332353966332D3463
64632D346636302D383639382D3137383965326438333832350000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572 
(Fri Apr 27 10:14:42 CEST 2012)
```

	Tag: 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: e3259cf3-4cdc-4f60-8698-1789e2d83825 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042 006B02000000040000000100000000420092090000000800000004F9A557242000D020000000400000 0001000000000042000F010000005842005C0500000004000000140000000042007F05000000040000000 000000000042007C0100000030420094070000002465333235396366332D346364632D346636302D38 3639382D313738396532643833383235000000000
13	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: 0x00000001 (1) Tag: 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: 3ddc1ae4-e212-46c7-a835-449fb94d12ff 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042 006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200 5C05000000040000001400000000420079010000003042009407000000243364646331616534 2D6532 31322D343663372D613833352D3434396662393464313266660000000

	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: 0x00000001 (1)
	    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572 (Fri Apr 27 10:14:42 CEST 2012)
	    Tag: 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: 3ddc1ae4-e212-46c7-a835-449fb94d12ff
	42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000100000000420092090000000800000004F9A557242000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000000000000042007C01000000304200940700000024336464633161653442D653231322D343663372D613833352D34343966623934643132666600000000

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

```
0x00000001 (1)

    Tag: 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: 25fc6fbe-
d7d3-4c8e-83ad-1879fa5990fa
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000484200
5C05000000040000001400000000420079010000003042009407000000243235666336666262652D6437
64332D346338652D383361642D31383739666135393930666100000000
```

Out: uuidCertificate

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572
(Fri Apr 27 10:14:42 CEST 2012)

    Tag: 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: 25fc6fbe-
d7d3-4c8e-83ad-1879fa5990fa
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B020000000400000001000000004200920900000008000000004F9A557242000D02000000040000
0001000000000042000F010000005842005C05000000040000001400000000042007F0500000004000000
0000000000042007C01000000304200940700000024323566633666662652D643764332D346338652D38
```

```
3361642D3138373966613539393066610000000
```

15

Destroy

In: uuidRecertifiedCertificate

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: 1d4786cd-
9d9a-41cb-90f7-bc0471c69779
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C0500000004000000140000000042007901000000304200940700000024316434373836636642D3964
39612D343163622D393066372D626330343731633639373739000000000
```

Out: uuidRecertifiedCertificate

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572
```

```
(Fri Apr 27 10:14:42 CEST 2012)

    Tag: 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: 1d4786cd-
9d9a-41cb-90f7-bc0471c69779



42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A557242000D02000000040000
0001000000000042000F01000000584200 5C0500000004000000140000000042007F0500000004000000
00000000000042007C01000000304200940700000024316434373836636 42D396439612D343163622D39
3066372D62633034373163363937373900000000
```

14 Key Wrapping

This section contains test cases that exercise the key wrapping functionality.

14.1 Test Case: Key Wrapping using AES Key Wrap and No Encoding

Register a 128-bit AES key encryption key (KEK) with the Cryptographic Usage Mask attribute set to Wrap and the Cryptographic Parameters specifying NIST Key Wrap as the Block Cipher Mode. Subsequently, register another 128-bit AES data key (Data Key). Retrieve the Data Key wrapped using the NIST Key Wrap algorithm and the KEK. The Encoding Option is set to No Encoding, which means that only the key material is wrapped as opposed to the whole TTLV-encoded Key Value structure being wrapped. Finally, destroy both keys to return the server to the initial state.

The key material for both the KEK and the Data Key in this test case are set to match the test vectors specified in Section 4.6 of [NISTKeyWrap]. This way, the wrapped key material returned in the Get response can be compared against the cipher text of the test vector in [NISTKeyWrap].

For a more detailed explanation of key wrapping and the use of the Cryptographic Parameters attribute and the Key Wrapping Specification and Key Wrapping Data structures, see [KMIP-UG].

Time	Request/Response messages
0	Register (symmetric key) In: objectType = '00000002', attributes={ CryptographicUsageMask='00000010', CryptographicParameters={ BlockCipherMode='0000000D' } }, keyEncryptionKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: Name

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

            Tag: Name Value (0x420055), Type: Text String (0x07), Data: AES-KEK

            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: 0x00000010
(Wrap Key)

        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:
0x0000000D (NISTKeyWrap)

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
000102030405060708090A0B0C0D0E0F

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

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



42007801000001904200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420000D0200000004000000010000000042000F01000001484200
5C0500000004000000030000000042007901000001304200570500000004000000020000000420091
01000000B84200080100000038420000A07000000044E616D650000000042000B01000000204200550 7
```

Out: uuidKEK

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572
(Fri Apr 27 10:14:42 CEST 2012)
    Tag: 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: 100182d5-
72b8-47aa-8383-4d97d512e98a
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A557242000D02000000040000
0001000000000042000F01000000584200 5C05000000040000000300000000042007F0500000004000000
0000000000042007C01000000304200940700000024313030313832643520373262382D343761612D38
3338332D3464393764353132653938610000000
```

1 Register (symmetric key)

In: objectType = '00000002', attributes={ CryptographicUsageMask='0000000C' }, dataKey

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: 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: Name

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

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

            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: 0x0000000C 
(Encrypt, Decrypt)

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 
00112233445566778899AABBCCDDEEFF

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

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



42007801000001504200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000001084200
5C0500000004000000030000000042007901000000F042005705000000040000000200000000420091
0100000078420008010000003842000A07000000044E616D650000000042000B010000002042005507
000000084145532D444617461420054050000000400000001000000004200080100000003042000A0700
00001843727970746F6772617068696320557361676520 4D61736B42000B02000000040000000C0000
000042008F010000005842004001000000504200420500000004000000010000000042004501000000
184200430800000010 00112233445566778899AABBCCDDEEFF420028050000000400000003000000000
42002A02000000040000008000000000
```

	Out: uuidDataKey
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
	    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572 (Fri Apr 27 10:14:42 CEST 2012)
	    Tag: 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: bff7347b-3a39-4ccb-8234-ba2560ca1598
	42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420 06B02000000040000000100000000420092090000000800000004F9A557242000D020000000400000001000000000042000F010000005842005C050000000400000003000000000042007F0500000004000000000000000042007C0100000030420094070000002462666637333437622D336133392D346363622D383233342D626132353630636131353938000000000

2	Get (symmetric key wrapped)
	In: uuidDataKey, KeyWrappingSpecification={ WrappingMethod='00000001', EncryptionKeyInformation={ UniqueIdentifier=uuidKEK, CryptographicParameters={ BlockCipherMode='0000000D' }, EncodingOption='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:
0x00000001 (1)

    Tag: 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: bff7347b-
3a39-4ccb-8234-ba2560ca1598

      Tag: Key Wrapping Specification (0x420047), Type: Structure (0x01), Data:

        Tag: Wrapping Method (0x42009E), Type: Enumeration (0x05), Data:
0x00000001 (Encrypt)

        Tag: Encryption Key Information (0x420036), Type: Structure (0x01), Data:

          Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data:
100182d5-72b8-47aa-8383-4d97d512e98a

          Tag: Cryptographic Parameters (0x42002B), Type: Structure (0x01), Data:

            Tag: Block Cipher Mode (0x420011), Type: Enumeration (0x05), Data:
0x0000000D (NISTKeyWrap)

        Tag: Encoding Option (0x4200A3), Type: Enumeration (0x05), Data:
0x00000001 (No Encoding)
```

```
42007801000001084200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000C04200
5C05000000040000000A00000000420079010000000A842009407000000246266663733437622D3361
33392D346363622D383233342D626132353630636131353938000000004200470100000007042009E05
00000004000000010000000042003601000000484200940700000024313030313832643532D37326238
2D343761612D383338332D3464393764353132653938610000000042002B010000001042001105000000
0004000000D000000004200A305000000040000000100000000
```

Out: objectType = '00000002', uuidDataKey, wrappedDataKey

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

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

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

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

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

```
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572
(Fri Apr 27 10:14:42 CEST 2012)

    Tag: 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: bff7347b-
3a39-4ccb-8234-ba2560ca1598

      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 (Raw)

          Tag: Key Value (0x420045), Type: Byte String (0x08), Data:
1FA68B0A8112B447AEF34BD8FB5A7B829D3E862371D2CFE5

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

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

          Tag: Key Wrapping Data (0x420046), Type: Structure (0x01), Data:

            Tag: Wrapping Method (0x42009E), Type: Enumeration (0x05), Data:
0x00000001 (Encrypt)

            Tag: Encryption Key Information (0x420036), Type: Structure (0x01),
Data:

              Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data:
100182d5-72b8-47aa-8383-4d97d512e98a

              Tag: Cryptographic Parameters (0x42002B), Type: Structure (0x01),
Data:

                Tag: Block Cipher Mode (0x420011), Type: Enumeration (0x05), Data:
0x0000000D (NISTKeyWrap)

            Tag: Encoding Option (0x4200A3), Type: Enumeration (0x05), Data:
0x00000001 (No Encoding)



42007B010000019842007A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A557242000D02000000040000
00010000000042000F010000014042005C05000000040000000A0000000042007F0500000004000000
000000000042007C0100000118420057050000000400000002000000004200940700000024626666 37
333437622D336133392D346363622D383233342D6261323536306361313539380000000042008F0100
0000D042004001000000C84200420500000004000000010000000042004508000000181FA68B0A8112
B447AEF34BD8FB5A7B829D3E862371D2CFE54200280500000004000000030000000042002A02000000
04000000800000000042004601000000704200 9E050000000400000001000000004200360100000048
```

```
42009407000000243130303138326435 2D373262382D343761612D383338332D346439376435313265
```

3 Get (symmetric key unwrapped)

In: uuidDataKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: 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: bff7347b-
3a39-4ccb-8234-ba2560ca1598
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000000A0000000042007901000000304200940700000024626666373334376 22D3361
33392D346363622D383233342D626132353630636131353938000000000
```

Out: objectType = '00000002', uuidDataKey, dataKey

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

```
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572 (Fri Apr 27 10:14:42 CEST 2012)
    Tag: 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: bff7347b-3a39-4ccb-8234-ba2560ca1598
      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 (Raw)
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 00112233445566778899AABBCCDDEEFF
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000080 (128)
```

```
42007B01000001204207A01000000484200690100000020420 6A02000000040000000100000000042
```

4

Destroy

In: uuidDataKey

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

```
0x00000001 (1)

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: 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: bff7347b-
3a39-4ccb-8234-ba2560ca1598
```

420078010000009042007701000000384200690100000020420006A020000000400000001000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
5C0500000004000000140000000042007901000000304200940700000024626666373334376 22D3361
33392D346363622D383233342D626132353630636131353938 00000000

Out: uuidDataKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572
(Fri Apr 27 10:14:42 CEST 2012)

    Tag: 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: bff7347b-
3a39-4ccb-8234-ba2560ca1598
```

42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A557242000D0200000004 0000

```
00010000000042000F01000000584200 5C050000000400000014000000000 42007F0500000004000000
```

```
0001000000000042000F010000005842005C05000000040000001400000000042007F0500000004000000
000000000042007C010000003042009407000000246266663733343762 2D336133392D346363622D38
3233342D62613235363063613135393800000000
```

5

Destroy

In: uuidKEK

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: 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: 100182d5-
72b8-47aa-8383-4d97d512e98a
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000001400000000420079010000003042009407000000243130303138326435 2D3732
62382D343761612D383338332D346439376435313265393861 00000000
```

Out: uuidKEK

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

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

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

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

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

	0x00000001 (1)
	
	    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572 (Fri Apr 27 10:14:42 CEST 2012)
	
	    Tag: 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: 100182d5-72b8-47aa-8383-4d97d512e98a
	
	42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000100000000420092090000000800000004F9A557242000D0200000004000000010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000000000000042007C0100000030420094070000002431303031383264352D373262382D343761612D383338332D34643937643531326539386100000000

14.2 Test Case: Key Wrapping using AES Key Wrap with Attributes

Register a 128-bit AES key encryption key (KEK) with the Cryptographic Usage Mask attribute set to Wrap and the Cryptographic Parameters specifying NIST Key Wrap as the Block Cipher Mode. Subsequently, register another 128-bit AES data key (Data Key). Retrieve the Data Key wrapped using the NIST Key Wrap algorithm and the KEK. The Cryptographic Usage Mask Attribute Name is specified, indicating to the server that this attribute is to be wrapped together with the key material. The Encoding Option field is omitted, which means that the default TTLV-encoding is used. Finally, destroy both keys to return the server to the initial state. For a more detailed explanation of key wrapping and the use of the Cryptographic Parameters attribute and the Key Wrapping Specification and Key Wrapping Data structures, see [KMIP-UG].

Time	Request/Response messages
0	Register (symmetric key) In: objectType = '00000002', attributes={ CryptographicUsageMask='00000010', CryptographicParameters={ BlockCipherMode='0000000D' } }, keyEncryptionKey Tag: Request Message (0x420078), Type: Structure (0x01), Data:

```
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
    Tag: 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: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: AES-KEK
            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: 0x00000010 (Wrap Key)
        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: 0x0000000D (NISTKeyWrap)
      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 (Raw)
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 000102030405060708090A0B0C0D0E0F
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
```

```
0x00000080 (128)
```

```
42007801000001904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000001484200
5C05000000040000000300000000420079010000013042005705000000040000000200000000420091
01000000B84200080100000038420000A070000000044E616D6500000000042000B01000000020420055 07
0000000074145532D4B454B0042005405000000040000000100000000420008010000003042000A0700
00001843727970746F6772617068696320557361676520D61736B42000B0200000004000000100000
00004200080100000003842000A07000000184372797074 6F6772617068696320506172616D65746572
7342000B01000000104200110500000004000000D0000000042008F01000000584200400100000050
4200420500000000400000001000000004200450100000018420043080000000100001020304050607 08
090A0B0C0D0E0F4200280500000004000000030000000042002A02000000040000008000000000
```

Out: uuidKEK

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5572
(Fri Apr 27 10:14:42 CEST 2012)

    Tag: 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: f4b2b4c3-
4c19-4ecf-827a-011ca6057d3e
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A557242000D02000000040000
00010000000042000F010000005842005C0500000004000000030000000042007F0500000004000000
000000000042007C010000003042009407000000246634623262346333 2D346331392D346563662D38
3237612D303131636136303537643365 00000000
```

1

Register (symmetric key)

In: objectType = '00000002', attributes={ CryptographicUsageMask='0000000C' }, dataKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: Name
          Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data:
            Tag: Name Value (0x420055), Type: Text String (0x07), Data: AES-Data
            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: 0x0000000C 
(Encrypt, Decrypt)
      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 (Raw)
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 
00112233445566778899AABBCCDDEEFF
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 
0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
```

```
0x00000080 (128)
```

```
42007801000001504200770100000038420069010000002042006A020000000400000001000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000001084200
5C0500000004000000030000000042007901000000F042005705000000040000000200000000420091
01000000784200080100000038420000A07000000044E616D6500000000042000B01000000204200550 7
```

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5573
(Fri Apr 27 10:14:43 CEST 2012)
    Tag: 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: 65b1481f-
3f3a-457f-9ba9-bb6f6814be70
```

```
42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000042
006B020000000400000001000000004200920900000008000000004F9A557342000D020000000400000
0001000000000042000F01000000584200 5C0500000004000000030000000042007F05000000040000000
00000000042007C01000000304200940700000024363562313438316 62D336633612D343537662D39
6261392D62623666363831346265373000000000
```

2 Get (symmetric key wrapped)

In: uuidDataKey, KeyWrappingSpecification={ WrappingMethod='00000001', EncryptionKeyInformation={ UniqueIdentifier=uuidKEK, CryptographicParameters={ BlockCipherMode='0000000D' }, AttributeNames={ 'Cryptographic Usage Mask' } } }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: 65b1481f-
3f3a-457f-9ba9-bb6f6814be70
      Tag: Key Wrapping Specification (0x420047), Type: Structure (0x01), Data:
        Tag: Wrapping Method (0x42009E), Type: Enumeration (0x05), Data: 
0x00000001 (Encrypt)
        Tag: Encryption Key Information (0x420036), Type: Structure (0x01), Data:
          Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 
f4b2b4c3-4c19-4ecf-827a-011ca6057d3e
          Tag: Cryptographic Parameters (0x42002B), Type: Structure (0x01), Data:
            Tag: Block Cipher Mode (0x420011), Type: Enumeration (0x05), Data: 
0x0000000D (NISTKeyWrap)
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: 
Cryptographic Usage Mask
```

```
42007801000001184200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000D04200
5C05000000040000000A00000000420079010000000B8420094070000002436356231343831662D3366
33612D343537662D396261392D626236663638313462653730000000000420047010000008042009E05
000000040000000100000000420036010000004842009407000000246634623262346332D34633139
2D346563662D383237612D303131636136303537643365000000000042002B01000000104200110500000
00040000000D000000000042000A07000000184372797074677261706869632055736167652D4D6173
6B
```

Out: objectType = '00000002', uuidDataKey, wrappedDataKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5573
(Fri Apr 27 10:14:43 CEST 2012)

    Tag: 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: 65b1481f-
3f3a-457f-9ba9-bb6f6814be70

      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 (Raw)

          Tag: Key Value (0x420045), Type: Byte String (0x08), Data:
0DC0F8CB416E7B4422D85805D3DD80E49C6C75F763D1BE99748DE568E4EECDC05B94B1C1946FD3DEF1
4CFE184DAADA0DAF07C93E038CEB9F501BDD8A82C7D6B33152DBF9D415924B9F13F6CB75FF880AB09D
C862E473F74BDAF9398EC7695D41

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

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

          Tag: Key Wrapping Data (0x420046), Type: Structure (0x01), Data:

            Tag: Wrapping Method (0x42009E), Type: Enumeration (0x05), Data:
0x00000001 (Encrypt)

            Tag: Encryption Key Information (0x420036), Type: Structure (0x01),
Data:

              Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data:
f4b2b4c3-4c19-4ecf-827a-011ca6057d3e

              Tag: Cryptographic Parameters (0x42002B), Type: Structure (0x01),
```

	Data: Tag: Block Cipher Mode (0x420011), Type: Enumeration (0x05), Data: 0x0000000D (NISTKeyWrap) 42007B01000001D042007A0100000048420069010000002042006A02000000040000000100000000042 006B0200000000400000001000000004200920900000008000000004F9A557342000D02000000040000 0001000000000042000F010000017842005C0500000004000000A000000042007F0500000004000000 0000000000042007C010000015042005705000000040000000200000000420094070000002436356231 343831662D336633612D343537662D396261392D626236663638313462653730000000042008F0100 00010842004001000001004200420500000000400000001000000004200450800000600DC0F8CB416E 7B4422D85805D3DD80E49C6C75F763D1BE99748DE568E4EECDC05B94B1C1946FD3DEF14CFE184DAADA 0DAF07C93E038CEB9F501BDD8A82C7D6B33152DBF9D415924B9F13F6CB75FF880AB09DC862E473F74B DAF9398EC7695D414200280500000000400000003000000042002A0200000000400000080000000042 004601000000604200 9E05000000040000000100000000420036010000004842009407000000246634 6232623463332D346331392D346563662D383237612D303131636136303537643365000000042002B 0100000010420011050000000040000000D00000000
3	Get (symmetric key unwrapped) In: uuidDataKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: 65b1481f-3f3a-457f-9ba9-bb6f6814be70 42007801000000904200770100000038420069010000002042006A02000000040000000100000000042 006B02000000004000000010000000042000D0200000000400000001000000042000F01000000484200 5C050000000400000000A00000000420079010000003042009407000000243635623134383166 2D3366 33612D343537662D396261392D626236663638313462653730000000000 Out: objectType = '00000002', uuidDataKey, dataKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5573
(Fri Apr 27 10:14:43 CEST 2012)

    Tag: 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: 65b1481f-
3f3a-457f-9ba9-bb6f6814be70

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
00112233445566778899AABBCCDDEEFF

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

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

```
42007B010000012042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A557342000D02000000040000
0001000000000042000F01000000C842005C0500000004000000A000000042007F0500000004000000
000000000042007C01000000A0420057050000000400000002000000004200940700000024363562 31
343831662D336633612D343537662D396261392D626236663638313462653730000000000042008F0100
00005842004001000000504200420500000004000000010000000042004501000000184200430800000
00100011223344556677889 9AABBCCDDEEFF42002805000000040000000300000000042002A02000000
04000000800000000
```

4

Destroy

In: uuidDataKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: 65b1481f-
3f3a-457f-9ba9-bb6f6814be70
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000484200
5C05000000040000001400000000420079010000003042009407000000243635623134383166 2D3366
33612D343537662D396261392D626236663638313462653730000000000
```

Out: uuidDataKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5573 
(Fri Apr 27 10:14:43 CEST 2012)
```

	Tag: 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: 65b1481f-3f3a-457f-9ba9-bb6f6814be70 42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042 006B02000000004000000010000000042009209000000080000000004F9A557342000D02000000040000 00010000000042000F010000005842005C050000000400000014000000000042007F0500000004000000 000000000042007C0100000030420094070000002436356231343831662D336633612D343537662D39 6261392D6262366636383134626537300000000
5	Destroy In: uuidKEK Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: f4b2b4c3-4c19-4ecf-827a-011ca6057d3e 420078010000009042007701000000384200690100000020042006A02000000040000000100000000042 006B0200000000400000001000000000042000D020000000400000001000000000042000F01000000484200 5C05000000040000001400000000420079010000003042009407000000246634623262346332D3463 31392D346563662D383237612D30313163613630353764336500000000

Out: uuidKEK

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5573 
(Fri Apr 27 10:14:43 CEST 2012)
    Tag: 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: f4b2b4c3-
4c19-4ecf-827a-011ca6057d3e
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A557342000D02000000040000
0001000000042000F010000005842005C0500000004000000140000000042007F0500000004000000
000000000042007C010000003042009407000000246634623262346332D346331392D346563662D38
3237612D3031316361363035376433650000000
```

15 Groups

This section contains test cases that exercise the group functionality.

15.1 Test Case: Locate a Fresh Object from the Default Group

Locate a single fresh object from the default object group. Perform a Get Attribute to retrieve the value of the Fresh attribute to make sure that the key is fresh. Get the object (the kind of object returned depends on the server policy), and get the Fresh attribute again to verify that the object is no longer fresh. Finally, destroy the object.

As with all other test cases, this example illustrates only one possible behavior related to the default group. In this example, it is assumed that the server has fresh objects available in the default group, or that it creates a new object on-the-fly as a consequence of the Locate request. It is also assumed that no other client retrieves the object after the Locate but before the batched Get Attributes request, thereby toggling the value of the Fresh attribute.

Time	Request/Response messages

0	Locate, Get Attributes
	In (header): batchOrderOption=’TRUE’
	In: maximumItems='00000001', objectGroupMember='00000001', attributes={ ObjectGroup='default' }
	In: <no Unique Identifier>, attributeNames={ 'Fresh' }
	`Tag: Request Message (0x420078), Type: Structure (0x01), Data:`
	`  Tag: Request Header (0x420077), Type: Structure (0x01), Data:`
	`    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)`
	`    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: Byte String (0x08), Data:`

```
1E766D8A95D6E5D1

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

      Tag: Maximum Items (0x42004F), Type: Integer (0x02), Data: 0x00000001 (1)

      Tag: Object Group Member (0x4200AC), Type: Enumeration (0x05), Data: 
0x00000001 (Group Member Fresh)

      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: default

  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: Byte String (0x08), Data: 
8650F83BE5373722

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

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



42007801000001104200770100000048420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042001006000000080000000000000001420000D0200000004000
000020000000042000F01000000784200 5C0500000004000000080000000042009308000000081E766D
8A95D6E5D14200790100000050420004F0200000004000000010000000004200AC0500000004000000001
0000000042000801000000284200 0A070000000C4F626A6563742047726F75700000000042000B0700
00000764656661756C740042000F01000000384200 5C05000000040000000B000000004200930800000
00088650F83BE537372242007901000000104200 0A070000000546726573680000000
```

Out: uuidKey

Out: uuidKey, attributes={ Fresh=true }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5573 
(Fri Apr 27 10:14:43 CEST 2012)

    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: Byte String (0x08), Data: 
1E766D8A95D6E5D1
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 
(Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 2e592193-
c09b-4c3c-afda-2e68b57e8c3a
  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: Byte String (0x08), Data: 
8650F83BE5373722
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 
(Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 2e592193-
c09b-4c3c-afda-2e68b57e8c3a
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Fresh
        Tag: Attribute Value (0x42000B), Type: Boolean (0x06), Data: TRUE


42007B010000015842007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A557342000D02000000040000
00020000000042000F01000000068420005C050000000400000008000000004200930800000081E766D
8A95D6E5D142007F0500000004000000000000000042007C0100000030420094070000002432653539
```

1

Get (managed object)

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:
0x00000001 (1)

    Tag: 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: 2e592193-
c09b-4c3c-afda-2e68b57e8c3a
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000000A00000000420079010000003042009407000000243265353932313933 2D6330
39622D346333632D616664612D32653638623537653863336100000000
```

Out: uuidKey, managedObject

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5573
(Fri Apr 27 10:14:43 CEST 2012)

    Tag: 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: 2e592193-
c09b-4c3c-afda-2e68b57e8c3a

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
7FE09D434868AE14A0021AC19330F8D9226790D680E519F8AC25F42D72F60F0C

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000100 (256)
```

```
42007B010000013042007A0100000048420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000420092090000000800000004F9A557342000D020000000400000
00010000000042000F01000000D842005C05000000040000000A0000000042007F0500000000400000
0000000000042007C01000000B042005705000000040000000200000000420094070000002432653539
323139332D633039622D346333632D616664612D3265363862353765386333610000000042008F0100
0000684200400100000060420042050000000400000001000000004200450100000028420043080000
00207FE09D434868AE14A0021AC19330F8D9226790D680E519F8AC25F42D72F60F0C42002805000000
0400000003000000042002A02000000040000010000000000
```

2

Get Attributes

In: uuidKey, attributeNames={ 'Fresh' }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: 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: 2e592193-
c09b-4c3c-afda-2e68b57e8c3a

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

```
420078010000000A0420077010000003842006901000000020042006A02000000040000000100000000042
006B02000000040000000100000000042000D020000000400000001000000000042000F01000000584200
```

```
5C0500000004000000000B00000000042007901000000404200940700000024326535393231393332D6330
39622D346333632D616664612D32653638623537653863336100000000042000A07000000005467265 73
68000000
```

Out: uuidKey, attributes={ Fresh=false }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5573 
(Fri Apr 27 10:14:43 CEST 2012)
    Tag: 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: 2e592193-
c09b-4c3c-afda-2e68b57e8c3a
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Fresh
        Tag: Attribute Value (0x42000B), Type: Boolean (0x06), Data: FALSE
```

```
42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A557342000D0200000004000 0
000100000000042000F01000000080042005C05000000040000000B000000000042007F050000000400000 0
000000000042007C010000005842009407000000243265353932313933 2D633039622D346333632D61
6664612D32653638623537653863336100000000420008010000002042000A07000000054672657368
000000042000B06000000080000000000000000
```

3

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: 
0x00000001 (1)
    Tag: 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: 2e592193-
c09b-4c3c-afda-2e68b57e8c3a
```

```
42007801000000904200770100000038420069010000002042006A020000000400000001000000004
2
006B0200000004000000010000000042000D0200000004000000010000000042000F010000004842
00
5C0500000004000000140000000042007901000000304200940700000024326535393231393322D6330
39622D346333632D616664612D32653638623537653863336100000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5573 
(Fri Apr 27 10:14:43 CEST 2012)
    Tag: 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: 2e592193-c09b-4c3c-afda-2e68b57e8c3a 42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420006B02000000040000000100000000420092090000000800000004F9A557342000D0200000004000000010000000042000F01000000584200 5C0500000004000000140000000042007F0500000004000000000000000042007C010000003042009407000000243265353932313933 2D633039622D346333632D616664612D3265363862353765386333610000000

15.2 Test Case: Client-side Group Management

Register two symmetric keys, both with the same (non-default) Object Group name specified and the Fresh attribute set to true. Get the Fresh attribute from both keys to make sure it was set. Perform three batched Locate and Get requests to get a fresh key from the group. The first two requests should return both the registered keys, whereas the third request should return no key. To clean up, destroy both keys.

This test case assumes that the server supports and sets the Fresh attribute when requested to do so by the client.

Time	Request/Response messages
0	Register (symmetric key) In: objectType='00000002' (Symmetric Key), attributes={ CryptographicAlgorithm='00000003' (AES), Cryptographic-length='256', CryptographicUsageMask='0000000C', ObjectGroup='ClientFreshTest', Fresh='true' }, symmetricKey1 Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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 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: 0x00000100
(256)
        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: Object
Group
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data:
ClientFreshTest
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Fresh
          Tag: Attribute Value (0x42000B), Type: Boolean (0x06), Data: TRUE
      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 (Raw)
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
          Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data:
0x00000003 (AES)
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000100 (256)
```

```
42007801000001F0420077010000003842006901000000204200 6A0200000004000000010000000042
```

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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5573
(Fri Apr 27 10:14:43 CEST 2012)
    Tag: 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: d441954d-
9b5e-4d90-81e0-4b775328957c
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042009209000000080000000004F9A557342000D020000000400000
0001000000000042000F01000000584200 5C0500000004000000030000000042007F050000000400000 0
00000000042007C0100000030420094070000002464343431393534642D396235652D346439302D38
3165302D34623737353332383935376300000000
```

1	Register (symmetric key)

In: objectType=’00000002’ (Symmetric Key), attributes={ CryptographicAlgorithm=’00000003’ (AES),

CryptographicLength=’256’, CryptographicUsageMask=‘0000000C’, ObjectGroup='ClientFreshTest', Fresh='true' }, symmetricKey2

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
    Tag: 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 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: 0x00000100 (256)
        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: Object Group
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data:
ClientFreshTest

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

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

          Tag: Attribute Value (0x42000B), Type: Boolean (0x06), Data: TRUE

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
00112233445566778899AABBCCDDEEFF000102030405060708090A0B0C0D0E0F

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000100 (256)



42007801000001F042007701000000384200690100000020420006A020000000400000001000000042
006B02000000040000000100000000042000D020000000400000001000000042000F01000001A84200
5C050000000400000003000000004200790100000190420057050000000400000002000000000420091
0100000108420008010000003042000A07000000174372797074 6F677261706869632041 6C676F7269
```

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:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5573
```

	(Fri Apr 27 10:14:43 CEST 2012) Tag: 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: 902b310c-5267-4022-ad0f-b1f9d1cc47d4 42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000100000000420092090000000800000004F9A557342000D0200000004000000010000000042000F010000005842005C0500000004000000030000000042007F0500000004000000000000000042007C010000003042009407000000243930326233313063 2D353236372D343032322D616430662D6231663964316363343764340000000 0
2	Get Attributes In: uuidKey1, attributesNames={ 'Fresh' } Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: d441954d-9b5e-4d90-81e0-4b775328957c Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Fresh 42007801000000A0420077010000003842006901000000204200 6A0200000004000000010000000042006B0200000004000000010000000042000D0200000004000000010000000042000F010000005842005C050000000400000000B000000004200790100000040420094070000002464343431393534642D396235652D346439302D383165302D3462373735333238393537630000000042000A070000000546726573

```
68000000
```

Out: uuidKey1, attributes={ Fresh='true' }

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5573 (Fri Apr 27 10:14:43 CEST 2012)
    Tag: 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: d441954d-9b5e-4d90-81e0-4b775328957c
      Tag: Attribute (0x420008), Type: Structure (0x01), Data:
        Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Fresh
        Tag: Attribute Value (0x42000B), Type: Boolean (0x06), Data: TRUE
```

```
42007B01000000D842007A0100000048420069010000002042006A02000000040000000100000000420
06B02000000040000000100000000420092090000000800000004F9A557342000D02000000040000
00010000000042000F01000000804200 5C050000000400000000B000000000042007F05000000040000000
000000000042007C01000000584200940700000024643434313935346 42D396235652D346439302D38
3165302D346237373533323839353763000000000420008010000002042000A070000000546726573680
0000042000B06000000080000000000000001
```

3

Get Attributes

In: uuidKey2, attributesNames={ 'Fresh' }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: 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: 902b310c-
5267-4022-ad0f-b1f9d1cc47d4

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

```
42007801000000A04200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000584200
5C05000000040000000B000000004200790100000040420094070000002439303262333130632D3532
36372D343032322D616430662D62316639643163633437643400000000042000A070000000546726573
68000000
```

Out: uuidKey2, attributes={ Fresh='true' }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574
(Fri Apr 27 10:14:44 CEST 2012)

    Tag: 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: 902b310c-5267-4022-ad0f-b1f9d1cc47d4 Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Fresh Tag: Attribute Value (0x42000B), Type: Boolean (0x06), Data: TRUE 42007B01000000D842007A0100000048420069010000002042006A0200000004000000010000000042 006B020000000400000001000000004200920900000008000000004F9A557442000D02000000040000 00010000000042000F010000008042005C05000000040000000B0000000042007F0500000004000000 000000000042007C0100000058420094070000002439303262333130632D353236372D343032322D61 6430662D62316639643163633437643400000000420008010000002042000A07000000054672657368 00000042000B06000000080000000000000001
4	Locate and Get In (header): batchOrderOption='TRUE' In: MaximumItems=1, objectGroupMember='00000001', attributes={ ObjectGroup='ClientFreshTest' } 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: 0x00000001 (1) 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: Byte String (0x08), Data: 294FB5E3E93F8ECC Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Maximum Items (0x42004F), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Object Group Member (0x4200AC), Type: Enumeration (0x05), Data:

```
0x00000001 (Group Member Fresh)

      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:
ClientFreshTest

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
9DA79A935D4E4AE6

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



4200780100000108420077010000004842006901000000204200 6A0200000004000000010000000042
006B020000000400000001000000004200100600000008000000000000000142000D02000000040000
0002000000000042000F010000008042005C050000000400000008000000004200930800000008294FB5
E3E93F8ECC420079010000005842004F020000000400000001000000004200AC050000000400000001
000000004200080100000030 42000A070000000C4F626A6563742047726F75700000000042000B0700
00000F436C69656E744672657368546573740042000F010000002842005C05000000040000000A0000
00004200930800000008 9DA79A935D4E4AE64200790100000000
```

Out: uuidKey1

Out: objectType='00000002', uuidKey1, symmetricKey1

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574
(Fri Apr 27 10:14:44 CEST 2012)

    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: Byte String (0x08), Data:
294FB5E3E93F8ECC

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

```
(Success)

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: d441954d-9b5e-4d90-81e0-4b775328957c

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 9DA79A935D4E4AE6

    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: d441954d-9b5e-4d90-81e0-4b775328957c

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000100 (256)



42007B01000001B042007A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A557442000D02000000040000
00020000000042000F010000006842005C050000000400000008000000004200930800000008294FB5
E3E93F8ECC42007F0500000004000000000000000042007C0100000030420094070000002464343431
393534642D396235652D346439302D383165302D3462373735333238393537630000000042000F0100
0000E842005C05000000040000000A0000000042009308000000089DA79A935D4E4AE642007F050000
0004000000000000000042007C01000000B04200570500000004000000020000000042009407000000
2464343431393534642D396235652D346439302D383165302D34623737353332383935376300000000
42008F0100000068420040010000006042004205000000040000000100000000420045010000002842
00430800000020000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F4200
280500000004000000030000000042002A02000000040000010000000000
```

5 Locate and Get

In (header): batchOrderOption=’TRUE’

In: MaximumItems=1, objectGroupMember='00000001', attributes={ ObjectGroup='ClientFreshTest' }

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: 
0x00000001 (1)
    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: Byte String (0x08), Data: 
85E3E21D14D6DF1D
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Maximum Items (0x42004F), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Object Group Member (0x4200AC), Type: Enumeration (0x05), Data: 
0x00000001 (Group Member Fresh)
      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: 
ClientFreshTest
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
40FEAE5EC1BDA875
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data: null
```

```
42007801000001084200770100000048420069010000002042006A020000000400000001000000004 2
006B02000000040000000100000000420010060000000800000000000000000142000D02000000040000
00020000000042000F010000008042005C050000000400000008000000004200930800000000885E3E2
1D14D6DF1D42007901000000584200 4F020000000400000001000000004200AC0500000004000000 01
00000000420008010000003042000A070000000C4F626A6563742047726F75700000000042000B0700
00000F436C69656E7446726573685465737400 42000F010000002842005C05000000040000000A0000
000042009308000000 0840FEAE5EC1BDA8754200790100000000
```

Out: uuidKey2

Out: objectType='00000002', uuidKey2, symmetricKey2

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574
(Fri Apr 27 10:14:44 CEST 2012)
    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: Byte String (0x08), Data:
85E3E21D14D6DF1D
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000
(Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 902b310c-
5267-4022-ad0f-b1f9d1cc47d4
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
40FEAE5EC1BDA875
    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: 902b310c-
5267-4022-ad0f-b1f9d1cc47d4
      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 (Raw)
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
```

	00112233445566778899AABBCCDDEEFF000102030405060708090A0B0C0D0E0F Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000100 (256) 42007B01000001B042007A0100000048420069010000002042006A0200000004000000010000000042 006B02000000040000000100000000420092090000000800000004F9A557442000D020000000400000 0002000000000042000F01000000684200 5C050000000400000008000000004200930800000000885E3E2 1D14D6DF1D42007F0500000004000000000000000042007C010000003042009407000000243930326 2 333130632D353236372D343032322D616430662D623166396431636334376434000000000042000F0100 0000E842005C050000000400000000A00000000420093080000000840FEAE5EC1BDA87542007F050000 000400000000000000000042007C01000000B042005705000000040000000200000000420094070000000 24393032623331306 32D353236372D343032322D616430662D623166396431636334376434000000000 42008F01000000684200400100000060420042050000000400000001000000004200450100000028 42 0043080000002000112233445566778899AABBCCDDEEFF000102030405060708090A0B0C0D0E0F4200 2805000000040000000300000000 42002A020000000400000100000000 00
6	Locate and Get In (header): batchOrderOption=’TRUE’ In: MaximumItems=1, objectGroupMember='00000001', attributes={ ObjectGroup='ClientFreshTest' } 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: 0x00000001 (1) 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: Byte String (0x08), Data: 657339BDF375BFA2 Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Maximum Items (0x42004F), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Object Group Member (0x4200AC), Type: Enumeration (0x05), Data:

```
0x00000001 (Group Member Fresh)

      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:
ClientFreshTest

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
5713C4911444B36E

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

```
42007801000001084200770100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200100600000008000000000000000142000D02000000040000
00020000000042000F010000008042005C050000000400000008000000004200930800000008657339
BDF375BFA2420079010000005842004F020000000400000001000000004200AC050000000400000001
00000000420008010000003042000A070000000C4F626A6563742047726F757000000000042000B0700
00000F436C69656E744672657368546573740042000F010000002842005C05000000040000000A0000
000042009308000000085713C4911444B36E4200790100000000
```

Out: <empty Locate payload>

Out: Operation Failed, Invalid Field

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574
(Fri Apr 27 10:14:44 CEST 2012)

    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: Byte String (0x08), Data:
657339BDF375BFA2

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

	(Success) Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: null Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get) Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 5713C4911444B36E Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000001 (Operation Failed) Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x00000007 (Invalid Field) Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Unique Identifier is not defined 42007B010000010042007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000010000000042009209000000080000000004F9A557442000D0200000004000000020000000042000F010000003842005C0500000004000000080000000042009308000000008657339BDF375BFA242007F0500000004000000000000000042007C010000000042000F010000006842005C050000000400000000A0000000042009308000000085713C4911444B36E42007F050000000400000001000000000042007E05000000040000000700000000042007D07000000020556E697175652049646E7469666965722069732006E6F742064656666696E6564
7	Destroy 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: 0x00000001 (1) Tag: 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: d441954d-9b5e-4d90-81e0-4b775328957c 42007801000000904200770100000038420069010000002042006A0200000004000000010000000042

	006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
	5C050000000400000014000000004200790100000030420094070000002464343431393534642D3962
	35652D346439302D383165302D34623737353332383935376300000000
	
	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: 0x00000001 (1)
	    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574 (Fri Apr 27 10:14:44 CEST 2012)
	    Tag: 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: d441954d-9b5e-4d90-81e0-4b775328957c
	
	42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
	006B020000000400000001000000004200920900000008000000004F9A557442000D02000000040000
	00010000000042000F010000005842005C050000000400000014000000004200 7F0500000004000000
	000000000042007C01000000304200940700000024643434313935346 42D396235652D346439302D38
	3165302D34623737353332383935376300000000

8	Destroy 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: 
0x00000001 (1)
    Tag: 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: 902b310c-
5267-4022-ad0f-b1f9d1cc47d4
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
5C0500000004000000140000000042007901000000304200940700000024393032623331306 32D3532
36372D343032322D616430662D623166396431636334376434 00000000
```

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: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574 
(Fri Apr 27 10:14:44 CEST 2012)
    Tag: 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: 902b310c-
5267-4022-ad0f-b1f9d1cc47d4
```

	42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042 006B0200000000400000001000000004200920900000008000000004F9A557442000D020000000040000 00010000000042000F01000000584200 5C0500000004000000140000000042007F0500000004000000 000000000042007C0100000030420094070000002439303262333130632D353236372D343032322D61 6430662D623166396431636334376434000000000

15.3 Test Case: Default Object Group Member

This test case exercises the 'default' Object Group Member flag in the Locate request. Three keys are created on the server and put into the same group (the Object Group attribute is set to the same value for all keys). Thereafter, the client performs four batched Locate and Get requests, asking for the default object from the group. This test case assumes that the server policy is such that it serves objects from the group in a round-robin fashion. The pointer to the default object is advanced each time an object is retrieved using a Get request. The first three times Locate and Get is executed, the three keys are returned one after the other. When Locate and Get is executed for the fourth time, the first key is again returned. Finally, all keys are destroyed.

Time	Request/Response messages

0	Create (three symmetric keys)
	In: objectType=’00000002’ (Symmetric Key), attributes={ CryptographicAlgorithm=’00000003’ (AES), Cryptographic-length=’256’, CryptographicUsageMask=‘0000000C’, ObjectGroup='RoundRobinTestGroup' }
	In: objectType=’00000002’ (Symmetric Key), attributes={ CryptographicAlgorithm=’00000003’ (AES), Cryptographic-length=’256’, CryptographicUsageMask=‘0000000C’, ObjectGroup='RoundRobinTestGroup' }
	In: objectType=’00000002’ (Symmetric Key), attributes={ CryptographicAlgorithm=’00000003’ (AES), Cryptographic-length=’256’, CryptographicUsageMask=‘0000000C’, ObjectGroup='RoundRobinTestGroup' }
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:

```
0x00000001 (1)

    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000003 (3)

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
75E8BDB337AEC40E

    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: 0x00000100
(256)

        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: Object
Group

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

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
AC0E6E56E8D99F66

    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: 0x00000100 (256)
        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: Object Group
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: RoundRobinTestGroup
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)
    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 77E87D356BA09DA1
    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: 0x00000100 (256)
        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: Object
```

```
Group
          Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data:
RoundRobinTestGroup
```

```
42007801000003D042007701000000384200690100000020420006A0200000004000000010000000042
006B02000000040000000100000000042000D020000000400000003000000042000F01000001284200
5C05000000040000000100000000420093080000000875E8BDB337AEC40E42007901000001004200057
050000000400000002000000004200910100000E842000801000000303042000A07000000174372797 0
```

```
42007801000003D0420077010000003842006901000000020420006A020000000400000001000000042
006B020000000400000001000000042000D02000000040000000300000000042000F01000001284200
5C0500000004000000010000000042009308000000875E8BDB337AEC40E42007901000001004200057
0500000004000000020000000042009101000000E842000801000000303042000A070000001743727970
746F6772617068696320416C676F726974686D0042000B0500000004000000030000000042000080100
00003042000A070000001443727970746F67726170686963204C656E6774680000000042000B020000
0004000000100000000042000801000000303042000A0700000018437279707467F677261706869632055
73616765204D61736B42000B0200000004000000C00000000420008010000003842000A070000000C
4F626A656374204772F75700000000042000B070000001352 6F756E64526F62696E5465737447726F
757000000000000042000F01000001284200 5C050000000400000001000000004200930800000008AC0E
6E56E8D99F664200790100000100420057050000000400000002000000004200910100000E8420008
0100000003042000A070000001743727970746F6772617068696320416C676F726974686D0042000B05
000000040000000300000000420008010000003042000A070000001443727970746F6772617068696 3
204C656E677468000000042000B020000000400000100000000004200080100000003042000A070000
00184372797074 6F67726170686963205573616765204D61736B42000B0200000004000000 0C000000
00420008010000003842000A070000000C4F626A656374204772 6F7570000000000042000B0700000013
526F756E64526F62696E5465737447726F75700000000000042000F0100000128420 05C050000000400
00000100000000420093080000000877E87D356BA09DA14200790100000100420057050000000040000
00020000000042009101000000E842000801000000303042000A070000001743727970746F6772617068
696320416C676F726974686D0042000B05000000040000000300000000420008010000003042000A07
000000144372797074 6F67726170686963204C656E677468000000042000B020000000400000100 00
0000004200080100000030 42000A07000000184372797074 6F677261706869632055736167 65204D61
736B42000B020000000400000 00C000000004200080100000038 42000A070000000C4F626A65637420
47726F7570000000000042000B070000001352 6F756E64526F62696E5465737447726F757000000000 00
```

Out: uuidKey1

Out: uuidKey2

Out: uuidKey3

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574
(Fri Apr 27 10:14:44 CEST 2012)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000003 (3)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000001 (Create)

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
75E8BDB337AEC40E

    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: 8d945322-
fd70-495d-bf7f-71481d1401f6

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
AC0E6E56E8D99F66

    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: 640e560a-
f396-48c5-ac13-53adfcc039e0

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
77E87D356BA09DA1

    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: 1d885eb6-
ee09-489a-8ba3-83823df63d8c
```

```
42007B01000001D042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A557442000D0200000004000
00030000000042000F010000007842005C0500000004000000010000000042009308000000875E8BD
B337AEC40E42007F0500000004000000000000000042007C010000004042005705000000040000002
00000000420094070000002438643934353332322D666437302D343935642D626637662D3731343831
643134303166360000000042000F010000007842005C0500000004000000010000000042009308000
0008AC0E6E56E8D99F6642007F0500000004000000000000000042007C01000000404200570500000
0400000002000000004200940700000024363430653536306612D663339362D343863352D616331332D
3533616466636330333965300000000042000F010000007842005C0500000004000000010000000042
009308000000877E87D356BA09DA142007F0500000004000000000000000042007C01000000404200
570500000004000000020000000042009407000000243164383835656236 2D656530392D343839612D
386261332D3833383233646636643863 00000000
```

1

Locate and Get (default key from group)

In (header): batchOrderOption=’TRUE’

In: maxItems='1', ObjectGroupMember='00000002', attributes={ ObjectGroup='RoundRobinTestGroup' }

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:
0x00000001 (1)
    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: Byte String (0x08), Data:
99E7A6EA0125BB67
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Maximum Items (0x42004F), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Object Group Member (0x4200AC), Type: Enumeration (0x05), Data:
0x00000002 (Group Member Default)
      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:
RoundRobinTestGroup
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
0EFD9C2E346EE1CB
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data: null
```

```
42007801000001104200770100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200100600000008000000000000000142000D02000000040000
00020000000042000F010000008842005C05000000040000000800000000420093080000000899E7A6
```

```
EA0125BB67420079010000006042004F020000000400000001000000004200AC050000000400000002
00000000420008010000003842000A070000000C4F626A6563742047726F75700000000042000B0700
000013526F756E64526F62696E546573744772 6F7570000000000042000F010000002842005C050000
00040000000A00000000420093080000000800EFD9C2E346EE1CB4200790100000000
```

Out: uuidKey1

Out: key1

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574
(Fri Apr 27 10:14:44 CEST 2012)

    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: Byte String (0x08), Data:
99E7A6EA0125BB67

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 8d945322-
fd70-495d-bf7f-71481d1401f6

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
0EFD9C2E346EE1CB

    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: 8d945322-
fd70-495d-bf7f-71481d1401f6
```

	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 (Raw) Tag: Key Value (0x420045), Type: Structure (0x01), Data: Tag: Key Material (0x420043), Type: Byte String (0x08), Data: BD13DA8BCE07EA6B89C4D110827BF6A8478CF95EDCA9BBC278AB04F4CBEECFF0 Tag: Cryptographic Algorithm (0x420028), Type: Enumeration (0x05), Data: 0x00000003 (AES) Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 0x00000100 (256) 42007B01000001B042007A0100000048420069010000002042006A0200000004000000010000000042 006B020000000400000001000000004200920900000008000000004F9A557442000D02000000040000 00020000000042000F010000006842005C05000000040000000800000000420093080000000899E7A6 EA0125BB6742007F0500000004000000000000000042007C0100000030420094070000002438643934 353332322D666437302D343935642D626637662D3731343831643134303166360000000042000F0100 0000E842005C05000000040000000A0000000042009308000000080EFD9C2E346EE1CB42007F050000 0004000000000000000042007C01000000B04200570500000004000000020000000042009407000000 2438643934353332322D666437302D343935642D626637662D37313438316431343031663600000000 42008F0100000068420040010000006042004205000000040000000100000000420045010000002842 00430800000020BD13DA8BCE07EA6B89C4D110827BF6A8478CF95EDCA9BBC278AB04F4CBEECFF04200 280500000004000000030000000042002A02000000040000010000000000
2	Locate and Get (default key from group) In (header): batchOrderOption='TRUE' In: maxItems='1', ObjectGroupMember='00000002', attributes={ ObjectGroup='RoundRobinTestGroup' } 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: 0x00000001 (1) 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: Byte String (0x08), Data: 
0303428F37F17B8D

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

      Tag: Maximum Items (0x42004F), Type: Integer (0x02), Data: 0x00000001 (1)

      Tag: Object Group Member (0x4200AC), Type: Enumeration (0x05), Data: 
0x00000002 (Group Member Default)

      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: 
RoundRobinTestGroup

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
DAE46B60D9B6459B

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

```
42007801000001104200770100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420010060000000800000000000000014200 0D0200000004000 0
```

Out: uuidKey2

Out: key2

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574 
(Fri Apr 27 10:14:44 CEST 2012)
```

```
    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: Byte String (0x08), Data: 
0303428F37F17B8D

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 640e560a-
f396-48c5-ac13-53adfcc039e0

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
DAE46B60D9B6459B

    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: 640e560a-
f396-48c5-ac13-53adfcc039e0

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 
430BFB0CBC273E15326E3A23965F7704A13AF37A642C37026C9A59694C83B7A3

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 
0x00000100 (256)
```

```
42007B01000001B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000000 4F9A557442000D020000000400 00
```

```
42007B01000001B042007A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A557442000D02000000040000
000200000000420000F0100000068420005C050000000400000008000000004200930800000008030342
8F37F17B8D42007F0500000004000000000000000042007C0100000030420094070000002436343065
353630612D663339362D343863352D616331332D3533616466636330333965300000000042000F0100
0000E842005C05000000040000000A000000004200930800000008DAE46B60D9B6459B42007F050000
000400000000000000000042007C01000000B04200570500000004000000020000000042009407000000
24363430653536 30612D663339362D343863352D616331332D353361646663633033396530000000
42008F010000006842004001000000604200420500000004000000010000000042004501000000 2842
004308000000 20430BFB0CBC273E15326E3A23965F7704A13AF37A642C37026C9A59694C83B7A34200
2805000000040000000300000000 42002A02000000040000010000000000
```

3	Locate and Get (default key from group) In (header): batchOrderOption='TRUE' In: maxItems='1', ObjectGroupMember='00000002', attributes={ ObjectGroup='RoundRobinTestGroup' } 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: 
0x00000001 (1)
    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: Byte String (0x08), Data: 
863C27D7A0D3DA5E
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Maximum Items (0x42004F), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Object Group Member (0x4200AC), Type: Enumeration (0x05), Data: 
0x00000002 (Group Member Default)
      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: 
RoundRobinTestGroup
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000A (Get)
    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
C4617B3205E96FB2
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data: null
```

```
42007801000001104200770100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200100600000008000000000000000142000D02000000040000
00020000000042000F010000008842005C050000000400000008000000004200930800000008863C27
```

```
D7A0D3DA5E420079010000006042004F020000000400000001000000004200AC050000000400000002
000000004200080100000003842000A070000000C4F626A6563742047726F7570000000000042000B0700
000013526F756E64526F62696E5465737447726F757000000000000042000F010000002842005C050000
00040000000A000000004200930800000008C4617B3205E96FB242007901000000000
```

Out: uuidKey3

Out: key3

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574
(Fri Apr 27 10:14:44 CEST 2012)

    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: Byte String (0x08), Data:
863C27D7A0D3DA5E

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1d885eb6-
ee09-489a-8ba3-83823df63d8c

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
C4617B3205E96FB2

    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: 1d885eb6-
ee09-489a-8ba3-83823df63d8c
```

```
      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
A51B38E400168A25F2F122D7B8543A00DAF022E61677A08A33A834F5F52C3097

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000100 (256)
```

```
42007B01000001B042007A0100000048420069010000002042006A0200000004000000010000000042
006B020000000400000001000000004200920900000008000000004F9A557442000D02000000040000
00020000000042000F010000006842005C050000000400000008000000004200930800000008863C27
D7A0D3DA5E42007F0500000004000000000000000042007C0100000030420094070000002431643838
356562362D656530392D343839612D386261332D3833383233646636336438630000000042000F0100
0000E842005C05000000040000000A000000004200930800000008C4617B3205E96FB242007F050000
0004000000000000000042007C01000000B04200570500000004000000020000000042009407000000
2431643838356562362D656530392D343839612D386261332D38333832336466363364386300000000
42008F0100000068420040010000006042004205000000040000000100000000420045010000002842
00430800000020A51B38E400168A25F2F122D7B8543A00DAF022E61677A08A33A834F5F52C30974200
280500000004000000030000000042002A02000000040000010000000000
```

4

Locate and Get (default key from group)

In (header): batchOrderOption=’TRUE’

In: maxItems='1', ObjectGroupMember='00000002', attributes={ ObjectGroup='RoundRobinTestGroup' }

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:
0x00000001 (1)

    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: Byte String (0x08), Data: 
F1CE9893EE5BDE19

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

      Tag: Maximum Items (0x42004F), Type: Integer (0x02), Data: 0x00000001 (1)

      Tag: Object Group Member (0x4200AC), Type: Enumeration (0x05), Data: 
0x00000002 (Group Member Default)

      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: 
RoundRobinTestGroup

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
9A18DD11CC6CE394

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

```
4200780100000110420077010000004842006901000000204200 6A020000000400000001000000000042
```

Out: uuidKey1

Out: key1

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574 
(Fri Apr 27 10:14:44 CEST 2012)
```

```
    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: Byte String (0x08), Data:
F1CE9893EE5BDE19

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 8d945322-
fd70-495d-bf7f-71481d1401f6

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
9A18DD11CC6CE394

    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: 8d945322-
fd70-495d-bf7f-71481d1401f6

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
BD13DA8BCE07EA6B89C4D110827BF6A8478CF95EDCA9BBC278AB04F4CBEECFF0

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000100 (256)
```

```
42007B01000001B042007A0100000048420069010000002042006A02000000040000000100000000 42
006B020000000400000001000000004200920900000008000000004F9A557442000D020000000400000
0002000000000042000F010000006842005C0500000004000000080000000042009308000000008F1CE98
93EE5BDE1942007F0500000004000000000000000042007C01000000304200940700000024386439 34
353332322D666437302D343935642D626637662D3731343831643134303166360000000042000F0100
0000E842005C05000000040000000A0000000042009308000000089A18DD11CC6CE39442007F050000
0004000000000000000042007C01000000B042005705000000040000000200000000420094070000 00
24386439343533323 22D666437302D343935642D626637662D37313438316431343031663600000000
42008F010000006842004001000000604200420500000004000000010000000042004501000000 2842
00430800000020BD13DA8BCE07EA6B89C4D110827BF6A8478CF95EDCA9BBC278AB04F4CBEECFF04200
280500000004000000030000000042002A02000000040000010000000000
```

5 Destroy

In: uuidKey1

In: uuidKey2

In: uuidKey3

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Batch Error Continuation Option (0x42000E), Type: Enumeration (0x05), 
Data: 0x00000001 (Continue)
    Tag: Batch Order Option (0x420010), Type: Boolean (0x06), Data: TRUE
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000003 (3)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 
(Destroy)
    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
F4CF0A5614786EB7
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 8d945322-
fd70-495d-bf7f-71481d1401f6
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 
(Destroy)
    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
DD55DA10EBE91928
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 640e560a-
f396-48c5-ac13-53adfcc039e0
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000014 
(Destroy)
    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data: 
18334AF52FEE87FA
```

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1d885eb6-
ee09-489a-8ba3-83823df63d8c
```

```
42007801000001804200770100000058420069010000002042006A02000000040000000100000000420
06B02000000040000000100000000042000E05000000040000000100000000420010060000000080000
00000000000142000D0200000004000000030000000042000F01000000584200 5C0500000004000000
```

Out: uuidKey1

Out: uuidKey2

Out: uuidKey3

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574
(Fri Apr 27 10:14:44 CEST 2012)

    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000003 (3)

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
F4CF0A5614786EB7

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 8d945322-
fd70-495d-bf7f-71481d1401f6
```

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
DD55DA10EBE91928

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 640e560a-
f396-48c5-ac13-53adfcc039e0

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

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

    Tag: Unique Batch Item ID (0x420093), Type: Byte String (0x08), Data:
18334AF52FEE87FA

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

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

      Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 1d885eb6-
ee09-489a-8ba3-83823df63d8c



42007B01000001A042007A0100000048420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042009209000000080000000004F9A557442000D0200000004000
000300000000042000F010000006842005C05000000040000001400000000420093080000000008F4CF0A
5614786EB742007F050000000400000000000000000042007C0100000030420094070000002438643934
353332322D666437302D343935642D626637662D37313438316431343031663600000000042000F0100
00006842005C050000000400000014000000004200930800000008DD55DA10EBE9192842007F050000
0004000000000000000042007C01000000304200940700000024363430653536303612D663339362D34
3863352D616331332D35336164666363303339653000000000042000F010000006842005C0500000004
000000140000000042009308000000818334AF52FEE87FA42007F050000000400000000000000000042
007C0100000030420094070000002431643838356562362D656530392D343839612D386261332D3833
38323364663633643863000000000
```

16 Discover Versions

This section contains a test case that exercises the functionality for discovering the KMIP versions supported.

16.1 Test Case: Discover Versions

Exercise the Discover Versions operation in different ways in order to find out which versions a server supports, as well as to get a list of versions supported by both client and server. The example server responses in this test case are based on a server which supports KMIP versions 1.1 and 1.0, with 1.1 being the preferred version.

Time	Request/Response messages

0	Discover Versions
	In: <no versions provided>
	`Tag: Request Message (0x420078), Type: Structure (0x01), Data:`
	`  Tag: Request Header (0x420077), Type: Structure (0x01), Data:`
	`    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)`
	`    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)`
	`  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:`
	`    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001E (Discover Versions)`
	`    Tag: Request Payload (0x420079), Type: Structure (0x01), Data: null`
	`42007801000000604200770100000038420069010000002042006A02000000040000000100000000042`
	`006B02000000040000000100000000042000D02000000040000000100000000042000F01000000184200`
	`5C05000000040000001E000000004200790100000000`
	Out: v1.1, v1.0
	`Tag: Response Message (0x42007B), Type: Structure (0x01), Data:`
	`  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:`

```
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004ED73ED7 (Thu Dec 01 09:46:15 CET 2011)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001E (Discover Versions)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 (Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
        Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
        Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
      Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
        Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
        Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000000 (0)
```

```
42007B01000000D042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004ED73ED742000D020000000040000
00010000000042000F010000007842005C0500000004000001E0000000042007F0500000004000000
000000000042007C010000005042006901000000020420006A020000000400000001000000042006B02
000000040000000100000000420069010000002042006A02000000040000000100000000042006B0200
000004000000000000000000
```

1

Discover Versions

In: v1.0

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

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

    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001E
(Discover Versions)

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

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

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

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



42007801000000884200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000404200
5C05000000040000001E000000004200790100000028420069010000002042006A0200000004000000
01000000042006B02000000040000000000000000
```

Out: v1.0

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004E048882
(Fri Jun 24 14:52:18 CEST 2011)

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

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

    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001E
(Discover Versions)

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

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

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

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

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



42007B01000000A842007A0100000048420069010000002042006A02000000040000000100000000042
```

```
006B020000000400000001000000004200920900000008000000004E04888242000D02000000040000
00010000000042000F010000005042005C05000000040000001E0000000042007F0500000004000000
000000000042007C0100000028420069010000002042006A02000000040000000100000000 42006B02
000000040000000000000000
```

2

Discover Versions

In: v1.1

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001E
(Discover Versions)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
        Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
        Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
```

```
42007801000000884200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000404200
5C05000000040000001E000000004200790100000028420069010000002042006A0200000004000000
010000000042006B0200000004000000010000000
```

Out: v1.1

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004ED73ED7
```

```
(Thu Dec 01 09:46:15 CET 2011)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001E
(Discover Versions)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000
(Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data:
      Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
        Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
        Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)


42007B01000000A842007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004ED73ED742000D02000000040000
00010000000042000F01000000005042005C050000000400000001E000000000042007F050000000400000000
000000000042007C010000002842006901000000002042006A02000000040000000100000000042006B02
0000000400000000100000000
```

3

Discover Versions

In: v9.31

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001E
(Discover Versions)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
        Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000009 (9)
        Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x0000001F (31)
```

```
42007801000000884200770100000038420069010000002042006A02000000040000000100000000042
006B02000000004000000010000000042000D02000000004000000010000000042000F01000000404200
5C05000000040000001E0000000042007901000000284200690100000020420060A0200000000400000000
09000000000042006B0200000000400000001F00000000
```

Out: <no versions>

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004ED73ED7 
(Thu Dec 01 09:46:15 CET 2011)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000001E 
(Discover Versions)
    Tag: Result Status (0x42007F), Type: Enumeration (0x05), Data: 0x00000000 
(Success)
    Tag: Response Payload (0x42007C), Type: Structure (0x01), Data: null
```

```
42007B010000008042007A0100000048420069010000002042006A02000000004000000010000000042
006B0200000000400000001000000004200920900000008000000004ED73ED742000D0200000000400000
0001000000000042000F010000002842005C05000000040000001E0000000042007F0500000000400000000
000000000042007C0100000000
```

17 Attribute Handling

This section contains test cases that demonstrate and exercise the usage of Attributes and Attribute Index values.

17.1 Test Case: Handling of Attributes and Attribute Index Values

This test case illustrates the changes in Attribute and Attribute Index handling introduced in KMIP v1.1. A symmetric key is created on the server, and two Name attributes and the Contact Information attribute is specified for the key. A Get Attributes request containing the Object Type attribute name twice is sent, but this operation fails since a single Attribute Name cannot be specified more than once in a Get Attributes request. The Object Type Attribute is then requested once, and this request succeeds. Thereafter, the Contact Information Attribute is modified, with the Attribute Index value of 0 specified. An attempt to delete the Name attribute without specifying the Attribute Index value fails. Finally, the created key is destroyed.

Time	Request/Response messages

0	Create (symmetric key)
	In: objectType='00000002' (Symmetric Key), attributes={ CryptographicAlgorithm='00000003' (AES), CryptographicLength='128', CryptographicUsageMask='0000000C', Name='FirstTestName', Name='SecondTestName', ContactInformation='admin@localhost' }
	`Tag: Request Message (0x420078), Type: Structure (0x01), Data:`
	`  Tag: Request Header (0x420077), Type: Structure (0x01), Data:`
	`    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)`
	`    Tag: 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: 0x00000100
(256)

        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:
FirstTestName

            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:
SecondTestName

            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:
admin@localhost



42007801000001F042007701000000384200690100000020420006A020000000400000001000000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000001A84200
5C0500000004000000010000000042007901000001904200570500000004000000020000000420091
0100000178420008010000003042000A07000000174372797074F6772617068696320416C676F7269
74686D0042000B05000000040000000300000000420008010000003042000A0700000014437279707 4
6F6772617068963204C656E67746800000000042000B02000000040000010000000000420008010000
003042000A0700000018437279707 46F677261706869632055736167652 04D61736B42000B02000000
040000000C000000004200080100000040420000A07000000044E616D650000000042000B0100000028
420055070000000D4669727374546573744E616D650000004200540500000004000000010000000042
000801000000040420000A07000000044E616D650000000042000B01000000284200550700000000E5365
```

	636F6E64546573744E616D65000042005405000000040000000100000000420008010000003842000A
	0700000013436F6E7461637420496E666F726D6174696F6E000000000042000B070000000F61646D69
	6E406C6F63616C686F737400
	
	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: 0x00000001 (1)
	    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574 (Fri Apr 27 10:14:44 CEST 2012)
	    Tag: 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: 28c7bad1-bc9b-41df-b439-1ba04a6fd982
	
	42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042
	006B02000000040000000100000000420092090000000800000004F9A557442000D02000000040000
	00010000000042000F010000006842005C0500000004000000010000000042007F0500000004000000
	000000000042007C010000004042005705000000040000000200000000420094070000002432386337
	626164312D626339622D343164662D623433392D316261303461366664393832000000000

1	Get attributes In: uuidKey, attributeNames={'ObjectType', 'ObjectType'} Tag: Request Message (0x420078), Type: Structure (0x01), Data:

```
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: 28c7bad1-
bc9b-41df-b439-1ba04a6fd982
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type
```

```
42007801000000C042007701000000384200690100000020042006A02000000040000000100000000042
006B020000000400000001000000042000D0200000004000000010000000042000F010000007842000
5C0500000004000000B00000000420079010000006042009407000000243238633762616431 2D6263
```

```
42007801000000C0420077010000003842006901000000204200 6A0200000004000000010000000042
```

Out: Operation Failed, Invalid Field

	(Operation Failed) Tag: Result Reason (0x42007E), Type: Enumeration (0x05), Data: 0x00000007 (Invalid Field) Tag: Result Message (0x42007D), Type: Text String (0x07), Data: Attribute Name specified more than once: Object Type 42007B01000000C842007A0100000048420069010000002042006A02000000040000000100000000042 006B02000000004000000010000000042009209000000008000000004F9A557442000D02000000040000 00010000000042000F01000000704200 5C050000000400000000B0000000042007F0500000004000000 01000000042007E0500000004000000070000000042007D07000000344174747269627574652004E61 6D6520737065636966696564206D6F7265207468616E206F6E63653A204F626A656374205479706500 000000
2	Get attributes In: uuidKey, attributeNames={‘ObjectType’} Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: 28c7bad1-bc9b-41df-b439-1ba04a6fd982 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Object Type 42007801000000A84200770100000038420069010000002042006A02000000040000000100000000042 006B02000000004000000010000000042000D0200000004000000010000000042000F0100000060420 0 5C050000000400000000B00000000420079010000004842009407000000243238633762616431 2D6263 39622D343164662D623433392D316261303461366664393832000000000042000A070000000B4F626A65 63742054797065000000000 Out: uuidKey, attribute={ ObjectType='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:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574
(Fri Apr 27 10:14:44 CEST 2012)
    Tag: 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: 28c7bad1-
bc9b-41df-b439-1ba04a6fd982
      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)
```

```
42007B01000000E042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A557442000D02000000040000
00010000000042000F01000000088842005C050000000400000000B000000042007F050000000040000000
0000000000042007C01000000604200940700000024323863376261643120626339622D343164662D62
3433392D3162613034613666643938320000000042000801000000002842000A070000000B4F626A6563
742054797065000000000042000B05000000040000000200000000
```

3

Modify attributes

In: uuidKey, attribute={ ContactInformation='donald@localhost' }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: 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: 28c7bad1-
bc9b-41df-b439-1ba04a6fd982

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

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

        Tag: Attribute Index (0x420009), Type: Integer (0x02), Data: 0x00000000 
(0)

        Tag: Attribute Value (0x42000B), Type: Text String (0x07), Data: 
donald@localhost
```

```
42007801000000E0420077010000003842006901000000204200 6A020000000400000001000000 0042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000984200
5C050000000400000000E00000000420079010000008042009407000000243238633762616431 2D6263
39622D343164662D623433392D316261303461366664393832000000000042000801000000484200 0A07
00000013436F6E7461637420496E666F726D6174696F6E00000000004200090200000004000000000
00000042000B070000001 0646F6E616C64406C6F63616C686F7374
```

Out: uuidKey, attribute={ ContactInformation='donald@localhost' }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574 
(Fri Apr 27 10:14:44 CEST 2012)

    Tag: 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: 28c7bad1-bc9b-41df-b439-1ba04a6fd982 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: donald@localhost 42007B01000000F042007A0100000048420069010000002042006A02000000040000000100000000042 006B02000000040000000100000000420092090000000800000004F9A557442000D02000000040000 00010000000042000F01000000098420005C05000000040000000E000000000042007F05000000004000000 0000000000042007C0100000070420094070000002432386337626164312D626339622D343164662D62 3433392D3162613034613666643938320000000042000801000000038420000A0700000013436F6E7461 637420496E666F726D6174696F6E000000000042000B0700000010646F6E616C64406C6F63616C686F 7374
4	Delete 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: 0x00000001 (1) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete Attribute) Tag: Request Payload (0x420079), Type: Structure (0x01), Data: Tag: Unique Identifier (0x420094), Type: Text String (0x07), Data: 28c7bad1-bc9b-41df-b439-1ba04a6fd982 Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Name

```
42007801000000A04200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F010000005842000
5C05000000040000000F00000000420079010000004042009407000000243238633762616431 2D6263
39622D343164662D623433392D316261303461366664393832000000000042000A07000000044E616D65
00000000
```

Out: Operation Failed, Invalid Field

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574
(Fri Apr 27 10:14:44 CEST 2012)

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

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

    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x0000000F (Delete
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: 28c7bad1-
bc9b-41df-b439-1ba04a6fd982

      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:
FirstTestName

          Tag: Name Type (0x420054), Type: Enumeration (0x05), Data: 0x00000001
(Uninterpreted Text String)
```

```
42007B01000000F842007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000004200920900000008000000004F9A557442000D0200000004000
0000100000000042000F01000000A042005C05000000040000000F0000000042007F050000000400000
000000000042007C0100000078420094070000002432386337626164312D626339622D343164662D62
3433392D3162613034613666643938320000000042000801000000404200 0A07000000044E616D6500
```

	00000042000B0100000028420055070000000D4669727374546573744E616D650000000420054050000 0004000000010000000

5	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: 0x00000001 (1)
	    Tag: 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: 28c7bad1-bc9b-41df-b439-1ba04a6fd982
	42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
	006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
	5C0500000004000000140000000042007901000000304200940700000024323863376261643122D6263
	39622D343164662D623433392D316261303461366664393832000000000
	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: 0x00000001 (1)

```
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5574
(Fri Apr 27 10:14:44 CEST 2012)

    Tag: 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: 28c7bad1-
bc9b-41df-b439-1ba04a6fd982



42007B01000000B042007A0100000048420069010000002042006A020000000400000001000000000042
006B020000000400000001000000004200920900000008000000004F9A557442000D02000000040000
00010000000042000F010000005842005C0500000004000000140000000042007F0500000004000000
000000000042007C0100000030420094070000002432386337626164312D626339622D343164662D62
3433392D3162613034613666643938320000000
```

18 Digest

This section contains test cases that exercises the Digest attribute.

18.1 Test Case: Digests of Symmetric Keys

Exercise the Digest attribute by registering two symmetric keys with the same key material but using different Key Format Type. The Digest Value for the key with the Key Format Type set to Transparent Symmetric Key is calculated on the TTLV-encoded Key Material structure (see [KMIP-Spec]

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof]), whereas the Digest Value for the key registered in the Raw Key Format Type is calculated on the raw Key Material Byte String. The server calculates the value of the mandatory Digest attribute instance using the Key Format Type used by the client when registering the keys. Thereafter, the client asks the server to create a symmetric key using the Create operation. In this situation, it is up to the server to choose what Key Format Type of the created key it uses to calculate the Digest Value. This test case assumes a server that does not compute any additional Digest Values using another Hashing Algorithm and/or Key Format Type.

Time	Request/Response messages

0	Register (symmetric key)
	In: objectType='00000002' (Symmetric Key), attributes={ CryptographicAlgorithm='00000003' (AES), Cryptographic-length='256', CryptographicUsageMask='0000000C', rawSymmetricKey
	`Tag: Request Message (0x420078), Type: Structure (0x01), Data:`
	`  Tag: Request Header (0x420077), Type: Structure (0x01), Data:`
	`    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:`
	`      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)`
	`      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)`
	`    Tag: 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 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: 0x00000100
(256)

        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: 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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
0000111122223333444455556666777788889999AAAABBBBCCCCDDDDEEEEFFFF

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000100 (256)
```

```
42007801000001904200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000001484200
5C0500000004000000030000000042007901000001304200570500000004000000020000000420091
01000000A8420008010000003042000A07000000174372797074F677261706869632041 6C676F7269
```

Out: uuidRawSymmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5575
(Fri Apr 27 10:14:45 CEST 2012)
    Tag: 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: 7b1b1baa-
d75a-41e8-a20a-b9e21604323b
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A557542000D020000000400000
000100000000042000F010000005842005C0500000004000000030000000042007F0500000004000000
000000000042007C010000003042009407000000243762316231626161612D643735612D343165382D61
3230612D62396532313630343332336200000000
```

1

Get Attributes

In: uuidRawSymmetricKey, attributeNames={ 'Digest' }

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

```
    Tag: 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: 7b1b1baa-d75a-41e8-a20a-b9e21604323b

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

```
42007801000000A042007701000000384200690100000020420006A02000000040000000100000000042
006B02000000004000000010000000042000D02000000004000000010000000042000F01000000584200
5C05000000040000000B000000004200790100000040420094070000002437623162316261612D6437
35612D343165382D613230612D623965323136303433323362000000000042000A070000000644696765
73740000
```

Out: uuidRawSymmetricKey, attributes={ Digest={ HashingAlgorithm='00000006', DigestValue='6C064FE051ADD11EDC07727B594EB48711DF843E08445BBA2CD786BC16BC58E8', KeyFormatType='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: 0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5575 (Fri Apr 27 10:14:45 CEST 2012)

    Tag: 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: 7b1b1baa-d75a-41e8-a20a-b9e21604323b

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

	Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digest Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Hashing Algorithm (0x420038), Type: Enumeration (0x05), Data: 0x00000006 (SHA-256) Tag: Digest Value (0x420035), Type: Byte String (0x08), Data: 6C064FE051ADD11EDC07727B594EB48711DF843E08445BBA2CD786BC16BC58E8 Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000001 (Raw) 42007B010000011842007A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000010000000042009209000000080000000004F9A557542000D0200000004000000010000000042000F01000000C042005C0500000004000000B0000000042007F0500000004000000000000000042007C01000000984200940700000024376231623162616 12D643735612D343165382D613230612D623965323136303433323362000000004200080100000060 42000A07000000064469676573740000042000B0100000048420038050000000400000006000000004200350800000020 6C064FE051ADD11EDC07727B594EB48711DF843E08445BBA2CD786BC16BC58E8420042050000000400000001000000 00
2	Register (symmetric key) In: objectType='00000002' (Symmetric Key), attributes={ CryptographicAlgorithm='00000003' (AES), Cryptographic-length='256', CryptographicUsageMask='0000000C', transparentSymmetricKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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 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: 0x00000100
(256)

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

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

          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data:
0x00000007 (Transparent Symmetric Key)

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

            Tag: Key Material (0x420043), Type: Structure (0x01), Data:

              Tag: Key (0x42003F), Type: Byte String (0x08), Data:
00001111222233334444555566667777888899999AAAABBBBCCCCDDDDEEEEFFFF

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000100 (256)



42007801000001984200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000001504200
5C05000000040000000300000000420079010000013842005705000000040000000200000000420091
01000000A84200080100000003042000A070000001743727970746F67726170686963204416C676F7269
74686D0042000B0500000004000000030000000042000801000000030042000A07000000144372797074
6F6772617068696320C4C656E67746800000000042000B020000000400000100000000004200080100000
003042000A070000001843727970746F6772617068696320557361676520D4D61736B42000B02000000
040000000C0000000042008F01000000704200400100000068420042050000000400000007000000000
42004501000000304200430100000028420003F080000002000011112222333344445555666677778888
889999AAAABBBBCCCCDDDDEEEEFFFF420028050000000400000003000000000042002A020000000040000
010000000000
```

Out: uuidTransparentSymmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5575
(Fri Apr 27 10:14:45 CEST 2012)
    Tag: 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: 4567027d-
d6d4-47cc-878e-9ec9d8d50db0
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A557542000D02000000040000
0001000000000042000F010000005842005C0500000004000000030000000042007F0500000004000000
000000000042007C01000000304200940700000024343536373032376442D643664342D343763632D38
3738652D3965633964386435306462300000000
```

3

Get Attributes

In: uuidTransparentSymmetricKey, attributeNames={ 'Digest' }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: 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: 4567027d-d6d4-47cc-878e-9ec9d8d50db0

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

```
42007801000000A0420077010000003842006901000000204200 6A02000000040000000100000000042
```

Out: uuidTransparentSymmetricKey, attributes={ Digest={ HashingAlgorithm='00000006', DigestValue='499CE96FF6F5E19FE9FE7A2FE4C3E92B88DB0001A4E8DF28D9966856B6C4B87C', KeyFormatType='00000007' } }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5575 (Fri Apr 27 10:14:45 CEST 2012)

    Tag: 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: 4567027d-d6d4-47cc-878e-9ec9d8d50db0

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

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

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

          Tag: Hashing Algorithm (0x420038), Type: Enumeration (0x05), Data: 0x00000006 (SHA-256)

          Tag: Digest Value (0x420035), Type: Byte String (0x08), Data: 499CE96FF6F5E19FE9FE7A2FE4C3E92B88DB0001A4E8DF28D9966856B6C4B87C
```

	Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000007 (Transparent Symmetric Key) 42007B010000011842007A0100000048420069010000002042006A02000000040000000100000000042006B0200000004000000010000000042009209000000080000000004F9A557542000D0200000004000000010000000042000F01000000C042005C0500000004000000000B000000042007F0500000004000000000000000042007C01000000984200940700000024343536373032376 42D643664342D343763632D383738652D39656339643864353064623000000000042000801000000060420000A070000000064469676573740000042000B01000000484200380500000004000000006000000004200350800000020499CE96FF6F5E19FE9FE7A2FE4C3E92B88DB0001A4E8DF28D9966856B6C4B87C42004205000000040000000700000000
4	Create (symmetric key) In: objectType = ‘00000002’, attributes={ CryptographicAlgorithm=’AES’, CryptographicLength=’256’, 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: 0x00000001 (1) Tag: 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: 0x00000100 (256)

```
        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)
```

```
42007801000001204200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000D84200
5C05000000040000000100000000420079010000000C0420057050000000400000002000000000420091
01000000A842000801000000304200A07000000174372797074 6F677261706869632041 6C676F7269
```

```
42007801000001204200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000D84200
5C0500000004000000010000000042007901000000C04200570500000004000000020000000042009 1
```

```
42007801000001204200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000D84200
5C050000000400000001000000004200790100000C0420057050000000400000002000000000420091
01000000A8420008010000003042000A07000000174372797074 6F6772617068696320416C676F7269
74686D0042000B05000000040000000300000000420008010000003042000A070000001443727970 74
6F6772617068696320 4C656E677468000000042000B02000000040000010000000000420008010000
003042000A070000001843727970746F677261706869632055736167652 04D61736B42000B02000000
040000000C00000000
```

Out: uuidCreatedSymmetricKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5575 
(Fri Apr 27 10:14:45 CEST 2012)

    Tag: 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: 99ef760d-
749d-4227-ade1-ca4984ce6cef
```

```
42007B01000000C042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A557542000D020000000400000
00010000000042000F010000006842005C0500000004000000010000000042007F05000000040000000
00000000042007C01000000404200570500000004000000020000000042009407000000243939656 6
```

```
373630642D373439642D343232372D616465312D636134393834636536636566600000000
```

5

Get Attributes

In: uuidCreatedSymmetricKey, attributeNames={ ‘Digest’ }

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: 99ef760d-
749d-4227-ade1-ca4984ce6cef
      Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digest
```

```
42007801000000A04200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000584200
5C05000000040000000B000000004200790100000040420094070000002439396566373630642D3734
39642D343232372D616465312D636134393834636536636566000000000042000A070000000644696765
73740000
```

Out: uuidCreatedSymmetricKey, attributes={ Digest={ HashingAlgorithm='00000006', DigestValue=*, KeyFormatType=serverChosenKeyFormatType } }

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

```
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5575 
(Fri Apr 27 10:14:45 CEST 2012)

    Tag: 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: 99ef760d-
749d-4227-ade1-ca4984ce6cef

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

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

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

          Tag: Hashing Algorithm (0x420038), Type: Enumeration (0x05), Data: 
0x00000006 (SHA-256)

          Tag: Digest Value (0x420035), Type: Byte String (0x08), Data: 
314B223505091DB03325C638A6016CF7080D3B116EB3F4896B6D24D4EC2215F8

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

```
42007B01000001184200７A0100000048420069010000002042006A0200000004000000010000000042
```

6 Get

In: uuidCreatedSymmetricKey, keyFormatType=serverChosenKeyFormatType

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

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

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

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

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

```
0x00000001 (1)

    Tag: 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: 99ef760d-
749d-4227-ade1-ca4984ce6cef

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

```
42007801000000A04200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000584200
5C05000000040000000A00000000420079010000004042009407000000243939656637363064 2D3734
39642D343232372D616465312D636134393834636536636566000000004200420500000004000000001
00000000
```

Out: uuidCreatedSymmetricKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5575
(Fri Apr 27 10:14:45 CEST 2012)

    Tag: 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: 99ef760d-
749d-4227-ade1-ca4984ce6cef

      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 (Raw)

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

            Tag: Key Material (0x420043), Type: Byte String (0x08), Data: 
C1A99AC4716D4EA787D40B449D7B816F0CE82772B463CBF3A042B3F8E81E7BB7

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data: 
0x00000100 (256)
```

```
42007B010000013042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A557542000D020000000400000
0001000000000042000F01000000D842005C0500000004000000000A0000000042007F0500000004000000
00000000000042007C01000000B042005705000000040000000200000000420094070000002439396566
373630642D373439642D343232372D616465312D6361343938346365366365660000000042008F0100
0000684200400100000060420042050000000400000001000000004200450100000028420043080000
0020C1A99AC4716D4EA787D40B449D7B816F0CE82772B463CBF3A042B3F8E81E7BB742002805000000
04000000030000000042002A020000000400000100000000
```

7 Destroy

In: uuidRawSymmetricKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: 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: 7b1b1baa-
d75a-41e8-a20a-b9e21604323b
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000000484200
5C050000000400000014000000004200790100000030420094070000002437623162316261612D6437
```

```
35612D343165382D613230612D62396532313630343332336200000000
```

Out: uuidRawSymmetricKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5575 
(Fri Apr 27 10:14:45 CEST 2012)
    Tag: 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: 7b1b1baa-
d75a-41e8-a20a-b9e21604323b
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000420
06B02000000040000000100000000420092090000000800000004F9A557542000D020000000400000
00010000000042000F010000005842005C0500000004000000140000000042007F050000000400000000
00000000042007C0100000030420094070000002437623162316261612D643735612D343165382D61
3230612D62396532313630343332336200000000
```

8 Destroy

In: uuidTransparentSymmetricKey

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: 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: 4567027d-
d6d4-47cc-878e-9ec9d8d50db0
```

```
42007801000000904200770100000038420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000042000D0200000004000000010000000042000F01000000484200
5C05000000040000001400000000420079010000003042009407000000243435363730323764 2D6436
64342D343763632D383738652D39656339643864353064623000000000
```

Out: uuidTransparentSymmetricKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5575 
(Fri Apr 27 10:14:45 CEST 2012)

    Tag: 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: 4567027d-
d6d4-47cc-878e-9ec9d8d50db0
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
```

```
006B020000000040000000010000000042009209000000008000000004F9A557542000D020000000400000
00010000000042000F010000005842005C050000000400000014000000000042007F0500000000400000000
000000000042007C0100000030420094070000002434353637303237642D643664342D343763632D38
3738652D396563396438643530646230000000000
```

9

Destroy

In: uuidCreatedSymmetricKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: 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: 99ef760d-
749d-4227-ade1-ca4984ce6cef
```

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000484200
5C05000000040000001400000000420079010000003042009407000000243939656637363064 2D3734
39642D343232372D616465312D636134393834636536636566 00000000
```

Out: uuidCreatedSymmetricKey

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

```
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5575
(Fri Apr 27 10:14:45 CEST 2012)

    Tag: 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: 99ef760d-
749d-4227-ade1-ca4984ce6cef



42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042009209000000080000000004F9A557542000D02000000040000
000100000000042000F01000000058420005C0500000004000000140000000042007F050000000400000000
00000000042007C01000000304200940700000024393965663736306442D373439642D343232372D61
6465312D636134393834636536636566600000000
```

18.2 Test Case: Digests of RSA Private Keys

Exercise the Digest attribute by registering two RSA private keys with the same key material but using different Key Format Type. The Digest Value for the key with the Key Format Type set to Transparent RSA Private Key is calculated on the TTLV-encoded Key Material structure (see [KMIP-Spec]

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof]), whereas the Digest Value for the key registered in the PKCS#1 Key Format Type is calculated on the Key Material Byte String. The server calculates the value of the mandatory Digest attribute instance using the Key Format Type used by the client when registering the keys. This test case assumes a server that does not compute any additional Digest Values using another Hashing Algorithm and/or Key Format Type.

Time	Request/Response messages
0	Register (private key) In: objectType='00000004' (Private Key), attributes={ CryptographicAlgorithm='00000004' (RSA), CryptographicLength='2048', CryptographicUsageMask='00000001', pkcs1PrivateKey

```
Tag: Request Message (0x420078), Type: Structure (0x01), Data:
  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data:
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)
    Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1)
  Tag: Batch Item (0x42000F), Type: Structure (0x01), Data:
    Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003
(Register)
    Tag: Request Payload (0x420079), Type: Structure (0x01), Data:
      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000004
(Private Key)
      Tag: Template-Attribute (0x420091), Type: Structure (0x01), Data:
        Tag: Attribute (0x420008), Type: Structure (0x01), Data:
          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data:
Cryptographic 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: 0x00000800
(2048)
        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:
0x00000003 (PKCS#1)
          Tag: Key Value (0x420045), Type: Structure (0x01), Data:
            Tag: Key Material (0x420043), Type: Byte String (0x08), Data:
308204A50201000282010100AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E44
0AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7
EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A411
00F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC829
5353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA8
```

```
09E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374
FE30E54951662A6EDA29C6FC411335D5DC7426B0F60502030100010282010003B12455D53C1816516C5
18493F6398AAFA72B17DFA894DB888A7D48C0A47F62579A4E644F86DA711FEC850CDD9DBBD17F69A44
3D2EC1DD60D3C618FA74CDE5FDAFABD6BAA26EB0A3ADB4DEF6480FB1218CD3B083E252E885B6F0729F
98B2144D2B72293E1B11D73393BC41F75B15EE3D7569B4995ED1A14425DA4319B7B26B0E8FEF17C375
42AE5C6D5849F87209567F3925A47B016D564859717BC57FCB4522D0AA49CE816E5BE7B3088193236E
C9EFFF140858045B73C5D79BAF38F7C67F04C5DCF0E3806AD982D1259058C3473E847179A878F2C6B3
BD968FB99EA46E9185892F3676E78965C2AED4877BA3917DF07C5E927474F19E764BA61DC38D63BF29
02818100D5C69C8C3CDC2464744A793713DAFB9F1DBC799FF96423FECD3CBA794286BCE920F4B5C183
F99EE9028DB6212C6277C4C8297FCFBCE7F7C24CA4C51FC7182FB8F4019FB1D5659674C5CBE6D5FA99
2051341760CD00735729A070A9E54D342BEBA8EF47EE82D3A01B04CEC4A00D4DDB41E35116FC221E85
4B43A696C0E6419B1B02818100CD5EA7702789064B673540CBFF09356AD80BC3D592812EBA47610B9F
AC6AECEFE22ACAE438459CDA74E59653D88C04189D34399BF5B14B920E34EF38A7D09FE69593396E8F
E735E6F0A6AE4990401041D8A406B6FD86A1161E45F95A3EAA5C1012E6662E44F15F335AC971E1766B
2BB9C985109974141B44D37E1E319820A55F02818100B2871237BF9FAD38C3316AB7877A6A868063E5
42A7186D431E8D27C19AC0414584033942E9FF6E2973BB7B2D8B0E94AD1EE82158108FBC8664517A5A
467FB963014BD5DCC2B4FB087C23039D11920DBE22FD9F16B4D89E23225CD455ADBAF32EF43F185864
A36D630309D6853F7714B39AAE1EBEE3938F87C2707E178C739F9F028181009690BED14B2AFAA26D98
6D592231EE27D71D49065BD2BA1F78157E20229881FD9D23227D0F8479EAEFA922FD75D5B16B1A561F
A6680B040CA0BDCE650B23B917A4B1BB7983A74FAD70E1C305CBEC2BFF1A85A726A1D90260E4F1084F
518234DCD3FE770B9520215BD543BB6A4117718754676A34171666A79F26E79C149C5AA102818100A0
C985A0A0A791A659F99731134C44F37B2E520A2CEA35800AD27241ED360DFDE6E8CA614F12047FD08B
76AC4D13C056A0699E2F98A1CAC91011294D71208F4ABAB33BA87AA0517F415BACA88D6BAC006088FA
601D349417E1F0C9B23AFFA4D496618DBC024986ED690BBB7B025768FF9DF8AC15416F489F8129C323
41A8B44F
```

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

          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000800 (2048)
```

```
42007801000006204200770100000038420069010000002042006A02000000040000000100000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000005D84200
5C0500000004000000030000000042007901000005C0420057050000000400000004000000000420091
01000000A84200080100000030420000A070000001743727970746F6772617068696320416C676F7269
74686D0042000B050000000400000004000000004200080100000030420000A0700000014437279707 4
6F6772617068696320C656E677468000000000042000B020000000400000800000000004200080100000
003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000
0400000001000000004200640100004F842004001000004F04200420500000004000000030000000 0
42004501000004B842004308000004A9308204A5020100028201 0100AB7F161C0042496CCD6C6D4DAD
B919973435357776003ACF54B7AF1E440AFB80B64A8755F8002CFEBA6B184540A2D66086D74648346D
75B8D71812B205387C0F6583BC4D7DC7EC114F3B176B7957C422E7D03FC6267FA2A6F89B9BEE9E60A1
D7C2D833E5A5F4BB0B1434F4E795A41100F8AA214900DF8B65089F98135B1C67B701675ABDBC7D5721
AAC9D14A7F081FCEC80B64E8A0ECC8295353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB66E3D211
26EBA8DA7D0CA34142CB76F91F013DA809E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CCE8946A9A
C99B1C2815C3612A29A82D73A1F99374FE30E54951662A6EDA29C6FC411335D5DC7426B0F605020301
0001028201003B12455D53C1816516C518493F6398AAFA72B17DFA894DB888A7D48C0A47F62579A4E6
44F86DA711FEC850CDD9DBBD17F69A443D2EC1DD60D3C618FA74CDE5FDAFABD6BAA26EB0A3ADB4DEF6
480FB1218CD3B083E252E885B6F0729F98B2144D2B72293E1B11D73393BC41F75B15EE3D7569B4995E
D1A14425DA4319B7B26B0E8FEF17C37542AE5C6D5849F87209567F3925A47B016D564859717BC57FCB
4522D0AA49CE816E5BE7B3088193236EC9EFFF140858045B73C5D79BAF38F7C67F04C5DCF0E3806AD9
82D1259058C3473E847179A878F2C6B3BD968FB99EA46E9185892F3676E78965C2AED4877BA3917DF0
7C5E927474F19E764BA61DC38D63BF2902818100D5C69C8C3CDC2464744A793713DAFB9F1DBC799FF9
6423FECD3CBA794286BCE920F4B5C183F99EE9028DB6212C6277C4C8297FCFBCE7F7C24CA4C51FC718
2FB8F4019FB1D5659674C5CBE6D5FA992051341760CD00735729A070A9E54D342BEBA8EF47EE82D3A0
1B04CEC4A00D4DDB41E35116FC221E854B43A696C0E6419B1B02818100CD5EA7702789064B673540CB
FF09356AD80BC3D592812EBA47610B9FAC6AECEFE22ACAE438459CDA74E59653D88C04189D34399BF5
B14B920E34EF38A7D09FE69593396E8FE735E6F0A6AE4990401041D8A406B6FD86A1161E45F95A3EAA
5C1012E6662E44F15F335AC971E1766B2BB9C985109974141B44D37E1E319820A55F02818100B28712
37BF9FAD38C3316AB7877A6A868063E542A7186D431E8D27C19AC0414584033942E9FF6E2973BB7B2D
8B0E94AD1EE82158108FBC8664517A5A467FB963014BD5DCC2B4FB087C23039D11920DBE22FD9F16B4
D89E23225CD455ADBAF32EF43F185864A36D630309D6853F7714B39AAE1EBEE3938F87C2707E178C73
```

```
9F9F028181009690BED14B2AFAA26D986D592231EE27D71D49065BD2BA1F78157E20229881FD9D2322
7D0F8479EAEFA922FD75D5B16B1A561FA6680B040CA0BDCE650B23B917A4B1BB7983A74FAD70E1C305
CBEC2BFF1A85A726A1D90260E4F1084F518234DCD3FE770B9520215BD543BB6A4117718754676A3417
1666A79F26E79C149C5AA102818100A0C985A0A0A791A659F99731134C44F37B2E520A2CEA35800AD2
7241ED360DFDE6E8CA614F12047FD08B76AC4D13C056A0699E2F98A1CAC91011294D71208F4ABAB33B
A87AA0517F415BACA88D6BAC006088FA601D349417E1F0C9B23AFFA4D496618DBC024986ED690BBB7B
025768FF9DF8AC15416F489F8129C32341A8B44F00000000000000420028050000000400000000400000
000042002A02000000040000080000000000
```

Out: uuidPkcs1PrivateKey

```
Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 
0x00000001 (1)
      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)
    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5575 
(Fri Apr 27 10:14:45 CEST 2012)
    Tag: 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: 214b43dc-
1ce7-47d7-9d7a-d91a6fd73c2b
```

```
42007B01000000B042007A0100000048420069010000002042006A0200000004000000010000000042
006B02000000040000000100000000420092090000000800000004F9A557542000D0200000004000000
0001000000000042000F010000005842005C0500000004000000030000000042007F0500000004000000
000000000042007C010000003042009407000000243231346234336463 2D316365372D343764372D39
6437612D643931613666643733633262 00000000
```

1

Get Attributes

In: uuidPkcs1PrivateKey, attributeNames={ ‘Digest’ }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: 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: 214b43dc-
1ce7-47d7-9d7a-d91a6fd73c2b

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

```
42007801000000A04200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000584200
5C05000000040000000B000000004200790100000040420094070000002432313462343364632D3163
65372D343764372D396437612D6439316136666437336332620000000042000A070000000644696765
73740000
```

Out: uuidPkcs1PrivateKey, attributes={ Digest={ HashingAlgorithm='00000006', DigestValue='11110A01ED4589D9987C9AD60368E2B762F2B20C00946E1932C1605A18172F55', KeyFormatType='00000003' } }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5575
(Fri Apr 27 10:14:45 CEST 2012)

    Tag: 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: 214b43dc-1ce7-47d7-9d7a-d91a6fd73c2b Tag: Attribute (0x420008), Type: Structure (0x01), Data: Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data: Digest Tag: Attribute Value (0x42000B), Type: Structure (0x01), Data: Tag: Hashing Algorithm (0x420038), Type: Enumeration (0x05), Data: 0x00000006 (SHA-256) Tag: Digest Value (0x420035), Type: Byte String (0x08), Data: 11110A01ED4589D9987C9AD60368E2B762F2B20C00946E1932C1605A18172F55 Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 0x00000003 (PKCS#1) 42007B01000001184200 7A0100000048420069010000002042006A0200000004000000010000000042006B0200000004000000010000000042009209000000080000000004F9A557542000D0200000004000000010000000042000F01000000C042005C0500000004000000 0B0000000042007F0500000004000000000000000042007C01000000984200940700000024323134623433646 32D316365372D343764372D39643761 2D643931613666643733633262000000004200080100000060 42000A070000000644696765737400004 2000B0100000048420038050000000400000006000000004200350800000020 11110A01ED4589D9987C9AD60368E2B762F2B20C00946E1932C1605A18172F554200420500000004000000030000000 0
2	Register (private key) In: objectType='00000004' (Private Key), attributes={ CryptographicAlgorithm='00000004' (RSA), CryptographicLength='2048', CryptographicUsageMask='00000001', transparentPrivateKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Count (0x42000D), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Batch Item (0x42000F), Type: Structure (0x01), Data: Tag: Operation (0x42005C), Type: Enumeration (0x05), Data: 0x00000003

```
(Register)

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

      Tag: Object Type (0x420057), Type: Enumeration (0x05), Data: 0x00000004
(Private Key)

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

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

          Tag: Attribute Name (0x42000A), Type: Text String (0x07), Data:
Cryptographic 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: 0x00000800
(2048)

        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:
0x0000000A (Transparent RSA Private Key)

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

            Tag: Key Material (0x420043), Type: Structure (0x01), Data:

              Tag: Modulus (0x420052), Type: Big Integer (0x04), Data:
00AB7F161C0042496CCD6C6D4DADB919973435357776003ACF54B7AF1E440AFB80B64A8755F8002CFE
BA6B184540A2D66086D74648346D75B8D71812B205387C0F6583BC4D7DC7EC114F3B176B7957C422E7
D03FC6267FA2A6F89B9BEE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA214900DF8B65089F
98135B1C67B701675ABDBC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C795328ABF70E1B42E
7BB8B7F4E8AC8C810CDB66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1B7AE64C54130FBC2
1D80E9C2CB06C5C8D7CCE8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E54951662A6EDA29C6
FC411335D5DC7426B0F605
(2164941877135146759475161971107567240550522517290336541039541410417068674050222298
5758086512196500456302881197402162582056963575786095048590601682011813501237136413
8418466855431722640135247520724017575039675157262400420544541648283972627275008078
1647083552529899699729330525936166381915418652119134873889823741153785842057990416
1751091557631352001731425721435127601318714216857056640324726857094534894545337269
6888419947625575843139335820123060872493739241201683398344443296661263702331951128
1344950307470516814970984794955227153388849763280329934582330150490464143489996260
076337716149243582343523430410910866919234 61)

              Tag: Private Exponent (0x420063), Type: Big Integer (0x04), Data:
3B12455D53C1816516C518493F6398AAFA72B17DFA894DB888A7D48C0A47F62579A4E644F86DA711FE
C850CDD9DBBD17F69A443D2EC1DD60D3C618FA74CDE5FDAFABD6BAA26EB0A3ADB4DEF6480FB1218CD3
B083E252E885B6F0729F98B2144D2B72293E1B11D73393BC41F75B15EE3D7569B4995ED1A14425DA43
19B7B26B0E8FEF17C37542AE5C6D5849F87209567F3925A47B016D564859717BC57FCB4522D0AA49CE
816E5BE7B3088193236EC9EFFF140858045B73C5D79BAF38F7C67F04C5DCF0E3806AD982D1259058C3
473E847179A878F2C6B3BD968FB99EA46E9185892F3676E78965C2AED4877BA3917DF07C5E927474F1
```

```
9E764BA61DC38D63BF29
(745706973685838578946126712174530767172551311553962755045647615831589914826887615
8582639566401239193216235126746176682996459367959367933668651657801650667092957780
5004573110535378012178323318556536420486996200625818559496541368747791032257508332
1620041215620177277215909683458659979150504394912393097515736311757114020599219959
8275556938537304302223619504767649529928402958490536347023158748753623556828429244
5148693873502200712082861995083783995720224553388380780283901622494150710167098487
9796050096943264010214343717760785867099769472998343832254180691121895373077720157
1643529497358482684822484513735382434823977)

               Tag: Public Exponent (0x42006C), Type: Big Integer (0x04), Data:
010001 (65537)

               Tag: P (0x42005E), Type: Big Integer (0x04), Data:
00D5C69C8C3CDC2464744A793713DAFB9F1DBC799FF96423FECD3CBA794286BCE920F4B5C183F99EE9
028DB6212C6277C4C8297FCFBCE7F7C24CA4C51FC7182FB8F4019FB1D5659674C5CBE6D5FA99205134
1760CD00735729A070A9E54D342BEBA8EF47EE82D3A01B04CEC4A00D4DDB41E35116FC221E854B43A6
96C0E6419B1B
(150118490317592161805840823662690407200298467544246751131465557870981954833124354
1343618778228061865402078826272567352686576901316720319872749178514538439404863823
3692588896294604518989434438249366184221901664624409044111533184368772164505320560
4787346257124478807067953590353906544790375145185063447686126363)

               Tag: Q (0x420071), Type: Big Integer (0x04), Data:
00CD5EA7702789064B673540CBFF09356AD80BC3D592812EBA47610B9FAC6AECEFE22ACAE438459CDA
74E59653D88C04189D34399BF5B14B920E34EF38A7D09FE69593396E8FE735E6F0A6AE4990401041D8
A406B6FD86A1161E45F95A3EAA5C1012E6662E44F15F335AC971E1766B2BB9C985109974141B44D37E
1E319820A55F
(144215537510067835554020354380136831606116996745325688732039749235544034597727381
7477792615433141141535897693998066286135187036907022650342065224770366925135971144
6982043208371025636968021721368115155920480397189283892640211360400033063619875371
4880263257665118610230510251577825517895327815044976174549738847)

               Tag: Prime Exponent P (0x420060), Type: Big Integer (0x04), Data:
00B2871237BF9FAD38C3316AB7877A6A868063E542A7186D431E8D27C19AC0414584033942E9FF6E29
73BB7B2D8B0E94AD1EE82158108FBC8664517A5A467FB963014BD5DCC2B4FB087C23039D11920DBE22
FD9F16B4D89E23225CD455ADBAF32EF43F185864A36D630309D6853F7714B39AAE1EBEE3938F87C270
7E178C739F9F
(125366359362987878721874271325857281787075017580361764135926903090417830690628637
6570145098970048277390194489230875441046874900986700944915931997028841773762418205
2401377586448876206247016742295589676497991974099493894948934536425031193608811810
0548030089852752637283308176353199858140012848789595305786187679)

               Tag: Prime Exponent Q (0x420061), Type: Big Integer (0x04), Data:
009690BED14B2AFAA26D986D592231EE27D71D49065BD2BA1F78157E20229881FD9D23227D0F8479EA
EFA922FD75D5B16B1A561FA6680B040CA0BDCE650B23B917A4B1BB7983A74FAD70E1C305CBEC2BFF1A
85A726A1D90260E4F1084F518234DCD3FE770B9520215BD543BB6A4117718754676A34171666A79F26
E79C149C5AA1
(105730627680298752806804858129862741428669445650844693718007322142750198732801398
2668919535320987618727082600686926299895074030689665750700147243843425698749304081
0604593009686299949723660034305738697402493890842588346637424286197122062969128459
4848206188935923508618880274773202320579744432263927479664401057)

               Tag: CRT Coefficient (0x420027), Type: Big Integer (0x04), Data:
00A0C985A0A0A791A659F99731134C44F37B2E520A2CEA35800AD27241ED360DFDE6E8CA614F12047F
D08B76AC4D13C056A0699E2F98A1CAC91011294D71208F4ABAB33BA87AA0517F415BACA88D6BAC0060
88FA601D349417E1F0C9B23AFFA4D496618DBC024986ED690BBB7B025768FF9DF8AC15416F489F8129
C32341A8B44F
(112908608227451761773934791220385463070083794319548451185931979476057892193890565
1176491525736015660620798423767272775497848711752178552898540389891048309628125936
9815417049156386009311432452536902841126400708503382950109367225764430639854207222
1929048307712709745630253031489375388035605164963430513223709775)

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

```
          Tag: Cryptographic Length (0x42002A), Type: Integer (0x02), Data:
0x00000800 (2048)
```

```
42007801000006684200770100000038420069010000002042006A020000000400000001000000000042
006B0200000004000000010000000042000D0200000004000000010000000042000F01000006204200
5C05000000040000000300000000420079010000006042005705000000040000000400000000420091
01000000A8420008010000003042000A07000000174372797074 6F6772617068696320416C676F7269
74686D0042000B05000000040000000400000000420008010000003042000A07000000144372797074
6F67726170686963204C656E6774680000000042000B02000000040000080000000000420008010000
003042000A070000001843727970746F67726170686963205573616765204D61736B42000B02000000
0400000001000000004200640100000540420040010000053842004205000000040000000A00000000
420045010000050042004301000004F842005204000001080000000000000000AB7F161C0042496CCD
6C6D4DADB919973435357776003ACF54B7AF1E440AFB80B64A8755F8002CFEBA6B184540A2D66086D7
4648346D75B8D71812B205387C0F6583BC4D7DC7EC114F3B176B7957C422E7D03FC6267FA2A6F89B9B
EE9E60A1D7C2D833E5A5F4BB0B1434F4E795A41100F8AA214900DF8B65089F98135B1C67B701675ABD
BC7D5721AAC9D14A7F081FCEC80B64E8A0ECC8295353C795328ABF70E1B42E7BB8B7F4E8AC8C810CDB
66E3D21126EBA8DA7D0CA34142CB76F91F013DA809E9C1B7AE64C54130FBC21D80E9C2CB06C5C8D7CC
E8946A9AC99B1C2815C3612A29A82D73A1F99374FE30E54951662A6EDA29C6FC411335D5DC7426B0F6
0542006304000001003B12455D53C1816516C518493F6398AAFA72B17DFA894DB888A7D48C0A47F625
79A4E644F86DA711FEC850CDD9DBBD17F69A443D2EC1DD60D3C618FA74CDE5FDAFABD6BAA26EB0A3AD
B4DEF6480FB1218CD3B083E252E885B6F0729F98B2144D2B72293E1B11D73393BC41F75B15EE3D7569
B4995ED1A14425DA4319B7B26B0E8FEF17C37542AE5C6D5849F87209567F3925A47B016D564859717B
C57FCB4522D0AA49CE816E5BE7B3088193236EC9EFFF140858045B73C5D79BAF38F7C67F04C5DCF0E3
806AD982D1259058C3473E847179A878F2C6B3BD968FB99EA46E9185892F3676E78965C2AED4877BA3
917DF07C5E927474F19E764BA61DC38D63BF2942006C0400000008000000000001000142005E040000
00880000000000000000D5C69C8C3CDC2464744A793713DAFB9F1DBC799FF96423FECD3CBA794286BC
E920F4B5C183F99EE9028DB6212C6277C4C8297FCFBCE7F7C24CA4C51FC7182FB8F4019FB1D5659674
C5CBE6D5FA992051341760CD00735729A070A9E54D342BEBA8EF47EE82D3A01B04CEC4A00D4DDB41E3
5116FC221E854B43A696C0E6419B1B42007104000000880000000000000000CD5EA7702789064B6735
40CBFF09356AD80BC3D592812EBA47610B9FAC6AECEFE22ACAE438459CDA74E59653D88C04189D3439
9BF5B14B920E34EF38A7D09FE69593396E8FE735E6F0A6AE4990401041D8A406B6FD86A1161E45F95A
3EAA5C1012E6662E44F15F335AC971E1766B2BB9C985109974141B44D37E1E319820A55F4200600400
0000880000000000000000B2871237BF9FAD38C3316AB7877A6A868063E542A7186D431E8D27C19AC0
414584033942E9FF6E2973BB7B2D8B0E94AD1EE82158108FBC8664517A5A467FB963014BD5DCC2B4FB
087C23039D11920DBE22FD9F16B4D89E23225CD455ADBAF32EF43F185864A36D630309D6853F7714B3
9AAE1EBEE3938F87C2707E178C739F9F42006104000000880000000000000000 9690BED14B2AFAA26D
986D592231EE27D71D49065BD2BA1F78157E20229881FD9D23227D0F8479EAEFA922FD75D5B16B1A56
1FA6680B040CA0BDCE650B23B917A4B1BB7983A74FAD70E1C305CBEC2BFF1A85A726A1D90260E4F108
4F518234DCD3FE770B9520215BD543BB6A4117718754676A34171666A79F26E79C149C5AA142002704
0000008800000000000000000A0C985A0A0791A659F99731134C44F37B2E520A2CEA35800AD27241ED
360DFDE6E8CA614F12047FD08B76AC4D13C056A0699E2F98A1CAC91011294D71208F4ABAB33BA87AA0
517F415BACA88D6BAC006088FA601D349417E1F0C9B23AFFA4D496618DBC024986ED690BBB7B025768
FF9DF8AC15416F489F8129C32341A8B44F4200280500000004000000040000000042002A0200000004
0000080000000000
```

Out: uuidTransparentPrivateKey

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

```
0x00000001 (1)

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5575 
(Fri Apr 27 10:14:45 CEST 2012)

    Tag: 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: 3a6d4b54-
f531-4c66-8041-f8b5c1b738aa
```

```
42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042
006B020000000400000001000000004200920900000008000000004F9A557542000D02000000040000
00010000000042000F010000005842005C0500000004000000030000000042007F0500000004000000
000000000042007C010000003042009407000000243361366434623534 2D663533312D346336362D38
3034312D66386235633162373338616100000000
```

3

Get Attributes

In: uuidTransparentPrivateKey, attributeNames={ ‘Digest’ }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: 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: 3a6d4b54-
f531-4c66-8041-f8b5c1b738aa

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

```
42007801000000A042007701000000384200690100000020420 06A020000000400000001000000004 2
```

Out: uuidTransparentPrivateKey, attributes={ Digest={ HashingAlgorithm='00000006', DigestValue='D73BBC51E83332935F912DBFC35C5EFC3B7BF8021835BA86B8DA4181F74244AC', KeyFormatType='0000000A' } }

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5575 
(Fri Apr 27 10:14:45 CEST 2012)

    Tag: 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: 3a6d4b54-
f531-4c66-8041-f8b5c1b738aa

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

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

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

          Tag: Hashing Algorithm (0x420038), Type: Enumeration (0x05), Data: 
0x00000006 (SHA-256)

          Tag: Digest Value (0x420035), Type: Byte String (0x08), Data: 
D73BBC51E83332935F912DBFC35C5EFC3B7BF8021835BA86B8DA4181F74244AC

          Tag: Key Format Type (0x420042), Type: Enumeration (0x05), Data: 
0x0000000A (Transparent RSA Private Key)
```

	42007B01000001184200 7A0100000048420069010000002042006A0200000004000000010000000042006B02000000040000000100000000420092090000000800000004F9A557542000D0200000004000000010000000042000F01000000C042005C0500000004000000000B000000000042007F0500000004000000000000000042007C01000000984200940700000024336136643462353 42D663533312D346336362D383034312D6638623563316237333861610000000042000801000000 6042000A0700000006446967657374000042000B01000000484200380500000004000000060000000042003508000000020D73BBC51E83332935F912DBFC35C5EFC3B7BF8021835BA86B8DA4181F74244AC420042050000000400000000A00000000

4	Destroy
	In: uuidTransparentPrivateKey
	Tag: Request Message (0x420078), Type: Structure (0x01), Data:
	  Tag: Request Header (0x420077), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:
	      Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1)
	      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1)
	    Tag: 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: 3a6d4b54-f531-4c66-8041-f8b5c1b738aa
	42007801000000904200770100000038420069010000002042006A0200000004000000010000000042006B02000000040000000100000000042000D0200000004000000010000000042000F010000004842005C0500000004000000140000000042007901000000304200940700000024336136643462353 42D663533312D346336362D383034312D66386235633162373338616100000000
	Out: uuidTransparentPrivateKey
	Tag: Response Message (0x42007B), Type: Structure (0x01), Data:
	  Tag: Response Header (0x42007A), Type: Structure (0x01), Data:
	    Tag: Protocol Version (0x420069), Type: Structure (0x01), Data:

	Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5576 (Fri Apr 27 10:14:46 CEST 2012) Tag: 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: 3a6d4b54-f531-4c66-8041-f8b5c1b738aa 42007B01000000B042007A0100000048420069010000002042006A02000000040000000100000000042 006B020000000400000001000000004200920900000008000000004F9A557642000D02000000040000 0001000000000042000F010000005842005C050000000400000014000000000042007F0500000004000000 000000000042007C010000003042009407000000243361366434623534 2D663533312D346336362D38 3034312D6638623563316237333861610000000
5	Destroy In: uuidPkcs1PrivateKey Tag: Request Message (0x420078), Type: Structure (0x01), Data: Tag: Request Header (0x420077), Type: Structure (0x01), Data: Tag: Protocol Version (0x420069), Type: Structure (0x01), Data: Tag: Protocol Version Major (0x42006A), Type: Integer (0x02), Data: 0x00000001 (1) Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data: 0x00000001 (1) Tag: 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: 214b43dc-1ce7-47d7-9d7a-d91a6fd73c2b

```
42007801000000904200770100000038420069010000002042006A02000000040000000100000000042
006B02000000040000000100000000042000D02000000040000000100000000042000F01000000484200
5C05000000040000001400000000420079010000003042009407000000243231346234336463 2D3163
65372D343764372D396437612D643931613666643733633262 00000000
```

Out: uuidPkcs1PrivateKey

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

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

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

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

      Tag: Protocol Version Minor (0x42006B), Type: Integer (0x02), Data:
0x00000001 (1)

    Tag: Time Stamp (0x420092), Type: Date-Time (0x09), Data: 0x000000004F9A5576
(Fri Apr 27 10:14:46 CEST 2012)

    Tag: 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: 214b43dc-
1ce7-47d7-9d7a-d91a6fd73c2b
```

```
42007B01000000B042007A01000000484200690100000020420006A02000000040000000100000000042
006B020000000400000001000000004200920900000008000000004F9A557642000D020000000400000
0001000000000042000F01000000584200 5C05000000040000001400000000042007F050000000400000000
000000000042007C010000003042009407000000243231346234336463 2D316365372D343764372D39
6437612D643931613666643733633262 00000000
```

19 Implementation Conformance

This document is intended to be informational only and as such has no conformance clauses. The conformance requirements for the KMIP Specification can be found in the "KMIP Specification" document itself (see [KMIP-Spec]

Key Management Interoperability Protocol Usage Guide Version 1.1. 01 December 2011. OASIS Standard. http://docs.oasis-open.org/kmip/spec/v1.1/cd01/kmip-spec-1.1-cd-01.doc

[KMIP-Prof]), at the URL noted on the cover page of this document.

Appendix 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:

Hal Aldridge, Sypris Electronics
Mike Allen, Symantec
Gordon Arnold, IBM
Todd Arnold, IBM
Matthew Ball, Oracle Corporation
Elaine Barker, NIST
Peter Bartok, Venafi, Inc.
Mathias Björkqvist, IBM
Kelley Burgin, National Security Agency
John Clark, Hewlett-Packard
Tom Clifford, Symantec Corp.
Graydon Dodson, Lexmark International Inc.
Chris Dunn, SafeNet, Inc.
Michael Duren, Sypris Electronics
Paul Earsy, SafeNet, Inc.
Stan Feather, Hewlett-Packard
Indra Fitzgerald, Hewlett-Packard

Alan Frindell, SafeNet, Inc.
Judith Furlong, EMC Corporation
Jonathan Geater, Thales e-Security
Susan Gleeson, Oracle Corporation
Robert Griffin, EMC Corporation
Paul Grojean, Individual
Robert Haas, IBM
Thomas Hardjono, M.I.T.
Steve He, Vormetric. Inc.
Kurt Heberlein, Hewlett-Packard
Joel Hockey, Cryptsoft Pty Ltd.
Larry Hofer, Emulex Corporation
Brandon Hoff, Emulex Corporation
Walt Hubis, NetApp
Tim Hudson, Cryptsoft Pty Ltd.
Jay Jacobs, Target Corporation
Glen Jaquette, IBM
Scott Kipp, Brocade Communications Systems, Inc.
Kathy Kriese, Symantec Corporation
David Lawson, Emulex Corporation
John Leiseboer, Quintenssence Labs
Hal Lockhart, Oracle Corporation
Robert Lockhart, Thales e-Security
Anne Luk, Cryptsoft Pty Ltd.
Shyam Mankala, EMC Corporation
Upendra Mardikar, PayPal Inc.
Luther Martin, Voltage Security
Hyrum Mills, Mitre Corporation
Bob Nixon, Emulex Corporation
René Pawlitzek, IBM
John Peck, IBM
Rob Philpott, EMC Corporation
Denis Pochuev, SafeNet, Inc.
Ajai Puri, SafeNet, Inc.
Peter Reed, SafeNet, Inc.
Bruce Rich, IBM
Warren Robbins, Credant Systems
Saikat Saha, SafeNet, Inc.
Subhash Sankuratripati, NetApp
Mark Schiller, Hewlett-Packard
Brian Spector, Certivox
Terence Spies, Voltage Security
Marcus Streets, Thales e-Security
Kiran Thota, VMware

Sean Turner, IECA, Inc.
Paul Turner, Venafi, Inc.
Marko Vukolić, EURECOM
Rod Wideman, Quantum Corporation
Steven Wierenga, Hewlett-Packard
Peter Yee, EMC Corporation
Krishna Yellepeddy, IBM
Michael Yoder, Vormetric. Inc.
Magda Zdunkiewicz, Cryptsoft Pty Ltd.
Peter Zelechoski, Election Systems & Software

559 # Appendix B Revision History

Revision	Date	Editor	Changes Made
wd-01	2011-07-13	Mathias Björkqvist	Updated document version from KMIP Version 1.0 to Version 1.1. Added new test cases for asymmetric keys and certificates, vendor extensions, key wrapping and version discovery. Addressed issues discovered since last document release.
wd-02	2011-07-28	Mathias Björkqvist	Corrected tag value for Encoding Option. Corrected name of Test Case 13.4. Replaced dates in the past with the current time in Test Case 9.2, corrected the Offset value and changed the test case description accordingly. Minor editorial changes.
wd-03	2011-08-18	Mathias Björkqvist	Corrected Certificate Link for the Public Key in Test Case 13.4, Time 9. Corrected order of Vendor Identification and Criticality Indicator fields in Message Extension in Test Cases 7.1 and 7.2. Added new Test Case 15.3 to exercise Object Group Member 'default'.
wd-04	2011-09-22	Mathias Björkqvist	Changed all protocol messages from v1.0 to v1.1. Corrected incorrect tag values in Test Case 3.1.3, Time 4 response. Corrected order of Unique Identifiers returned in Re-key Key Pair response in Test Case 13.3. Added Device Credential test case as Test Case 11.2.
wd-05	2011-10-06	Mathias Björkqvist	Updated the list of participants. Replaced Octet String with Byte String. Added Section for Attribute Index test case. Added symmetric key Digest test case as Test Case . Added clarifying text to Credential test cases.
wd-06	2011-10-17	Mathias Björkqvist	Added private key Digest test case as Test Case 18.2. Added second key wrapping test case as Test Case 14.2, changed both key wrapping test cases to use 128-bit wrapping keys.
wd-07	2011-12-01	Mathias Björkqvist	Applied new template. Modified existing test cases to always include the Attribute Index. Added new test case with Attribute and

			Attribute Index usage examples as Test Case 17.1. Minor editorial changes.
wd-08	2011-12-06	Mathias Björkqvist	Changed Device Credential to use new Device Serial Number tag.
Cnd-01	2012-1-4	OASIS admin	Committee Note Draft for Public Review
wd-09	2012-04-13	Mathias Björkqvist	Renamed document from Use Cases to Test Cases. Removed incorrect “Owner” attribute from Get Attribute List response in Test Cases 3.1.4, 4.1, 13.2 and 13.4. Added X.509 Certificate attributes to Get Attribute List response in Test Cases 13.2 and 13.4.
wd-10	2012-04-27	Mathias Björkqvist	Updated Test Cases according to latest Attribute Index proposal. Updated list of contributors.