



KMIP Storage Array with Self-Encrypting Drives Profile Version 1.0

Committee Specification Draft 01 / Public Review Draft 01

09 January 2014

Specification URIs

This version:

<http://docs.oasis-open.org/kmip/kmip-sa-sed-profile/v1.0/csprd01/kmip-sa-sed-profile-v1.0-csprd01.doc> (Authoritative)
<http://docs.oasis-open.org/kmip/kmip-sa-sed-profile/v1.0/csprd01/kmip-sa-sed-profile-v1.0-csprd01.html>
<http://docs.oasis-open.org/kmip/kmip-sa-sed-profile/v1.0/csprd01/kmip-sa-sed-profile-v1.0-csprd01.pdf>

Previous version:

N/A

Latest version:

<http://docs.oasis-open.org/kmip/kmip-sa-sed-profile/v1.0/kmip-sa-sed-profile-v1.0.doc>
(Authoritative)
<http://docs.oasis-open.org/kmip/kmip-sa-sed-profile/v1.0/kmip-sa-sed-profile-v1.0.html>
<http://docs.oasis-open.org/kmip/kmip-sa-sed-profile/v1.0/kmip-sa-sed-profile-v1.0.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:

Tim Hudson (tjh@cryptsoft.com), Cryptsoft Pty Ltd.
Mahadev Karadigudda (mahadev@netapp.com), NetApp

Related work:

This specification is related to:

- *Key Management Interoperability Protocol Profiles Version 1.0*. 01 October 2010. OASIS Standard. <http://docs.oasis-open.org/kmip/profiles/v1.0/os/kmip-profiles-1.0-os.html>.
- *Key Management Interoperability Protocol Specification Version 1.1*. 24 January 2013. OASIS Standard. <http://docs.oasis-open.org/kmip/spec/v1.1/os/kmip-spec-v1.1-os.html>.
- *Key Management Interoperability Protocol Specification Version 1.2*. Latest version. <http://docs.oasis-open.org/kmip/spec/v1.2/kmip-spec-v1.2.html>.

Abstract:

Describes a profile for Storage Arrays with Self-Encrypting Drives as KMIP clients interacting with KMIP servers.

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

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

Citation format:

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

[kmip-sa-sed-v1.0]

KMIP Storage Array with Self-Encrypting Drives Profile Version 1.0. Edited by Tim Hudson and Mahadev Karadigudda. 09 January 2014. OASIS Committee Specification Draft 01 / Public Review Draft 01. <http://docs.oasis-open.org/kmip/kmip-sa-sed-profile/v1.0/csprd01/kmip-sa-sed-profile-v1.0-csprd01.html>. Latest version: <http://docs.oasis-open.org/kmip/kmip-sa-sed-profile/v1.0/kmip-sa-sed-profile-v1.0.html>.

Notices

Copyright © OASIS Open 2014. All Rights Reserved.

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

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

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

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

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

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

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

The name "OASIS" is a trademark of [OASIS](#), the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/policies-guidelines/trademark> for above guidance.

Table of Contents

1	Introduction	5
1.1	Terminology	5
1.2	Normative References	5
1.3	Non-Normative References	6
2	Storage Array with Self-Encrypting Drives Profile	7
2.1	Authentication Suite	7
2.2	Storage Array with Self-Encrypting Drives	7
3	Storage Array with Self-Encrypting Drives Test Cases	9
3.1	Mandatory Test Cases	9
3.1.1	SASED-M-1-10 - Configuration	9
3.1.2	SASED-M-2-10 - Register the authentication key	10
3.1.3	SASED-M-3-10 - Retrieve Authentication Key	13
3.1.4	SASED-M-1-11 - Configuration	18
3.1.5	SASED-M-2-11 - Register the authentication key	19
3.1.6	SASED-M-3-11 - Retrieve Authentication Key	22
3.1.7	SASED-M-1-12 - Configuration	27
3.1.8	SASED-M-2-12 - Register the authentication key	28
3.1.9	SASED-M-3-12 - Retrieve Authentication Key	32
4	Conformance	38
4.1	Conformance Statement	38
4.2	Permitted Test Case Variations	38
4.2.1	Variable Items	38
4.2.2	Variable behavior	39
Appendix A.	Acknowledgments	41
Appendix B.	KMIP Specification Cross Reference	44
Appendix C.	Revision History	49

1 Introduction

For normative definition of the elements of KMIP see the [KMIP Specification](#) [KMIP-SPEC] and the [KMIP Profiles](#) [KMIP-PROF].

Illustrative guidance for the implementation of KMIP clients and servers is provided in the [KMIP Usage Guide](#) [KMIP-UG].

This profile defines the necessary KMIP functionality that a Storage Array with Self-Encrypting Drives operating as a KMIP client SHALL use and a KMIP server conforming to this profile SHALL support in order to interoperate in conformance with this profile.

1.1 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

Authentication Key	A secret used by self-encrypting drives to verify authenticity of the client before allowing the drive to perform sensitive operations.
--------------------	---

1.2 Normative References

- [RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- [RFC2246] T. Dierks and C. Allen, *The TLS Protocol, Version 1.0*, IETF RFC 2246, Jan 1999, <http://www.ietf.org/rfc/rfc2246.txt>
- [KMIP-SPEC] One or more of [KMIP-SPEC-1_0], [KMIP-SPEC-1_1], [KMIP-SPEC-1_2]
- [KMIP-SPEC-1_0] Key Management Interoperability Protocol Specification Version 1.0 <http://docs.oasis-open.org/kmip/spec/v1.0/os/kmip-spec-1.0-os.doc>
OASIS Standard, October 2010.
- [KMIP-SPEC-1_1] *Key Management Interoperability Protocol Specification Version 1.1.* <http://docs.oasis-open.org/kmip/spec/v1.1/os/kmip-spec-v1.1-os.doc>
OASIS Standard. 24 January 2013.
- [KMIP-SPEC-1_2] *Key Management Interoperability Protocol Specification Version 1.2.* [URL](#)
Candidate OASIS Standard 01. DD MMM YYYY.
- [KMIP-PROF] One or more of [KMIP-PROF-1_0], [KMIP-PROF-1_1], [KMIP-PROF-1_2]
- [KMIP-PROF-1_0] *Key Management Interoperability Protocol Usage Guide Version 1.0.* <http://docs.oasis-open.org/kmip/profiles/v1.0/os/kmip-profiles-1.0-os.doc>
OASIS Standard. 1 October 2010.
- [KMIP-PROF-1_1] *Key Management Interoperability Protocol Usage Guide Version 1.1.* <http://docs.oasis-open.org/kmip/profiles/v1.1/os/kmip-profiles-v1.1-os.doc>
OASIS Standard 01. 24 January 2013.
- [KMIP-PROF-1_2] *Key Management Interoperability Protocol Usage Guide Version 1.2.* [URL](#)
Candidate OASIS Standard 01. DD MMM YYYY.

1.3 Non-Normative References

- [KMIP-UG] One or more of [KMIP-UG-1_0], [KMIP-UG-1_1], [KMIP-UG-1_2]
[KMIP-UG-1_0] *Key Management Interoperability Protocol Usage Guide Version 1.0.*
<http://docs.oasis-open.org/kmip/ug/v1.1/kmip-ug-v1.1-cnd01.doc>
Committee Note Draft, 1 December 2011
- [KMIP-UG-1_1] *Key Management Interoperability Protocol Usage Guide Version 1.1.*
<http://docs.oasis-open.org/kmip/ug/v1.1/cn01/kmip-ug-v1.1-cn01.doc>
Committee Note 01, 27 July 2012
- [KMIP-UG-1_2] *Key Management Interoperability Protocol Usage Guide Version 1.2.*
[URL](#)
Committee Note Draft, DD MMM YYYY
- [KMIP-TC-1_1] *Key Management Interoperability Protocol Test Cases Version 1.1.*
<http://docs.oasis-open.org/kmip/testcases/v1.1/cn01/kmip-testcases-v1.1-cn01.doc>, Committee Note 01, 27 July 2012.
- [KMIP-TC-1_2] *Key Management Interoperability Protocol Test Cases Version 1.2.*
[URL](#), Committee Note Draft, DD MMM YYYY.
- [KMIP-UC] *Key Management Interoperability Protocol Use Cases Version 1.0.*
<http://docs.oasis-open.org/kmip/usecases/v1.0/cs01/kmip-usecases-1.0-cs-01.doc>, Committee Specification, 15 June 2010.

2 Storage Array with Self-Encrypting Drives Profile

The Storage Array with Self-Encrypting Drives Profile is a storage array containing self-encrypting drives operating as a KMIP client interacting with a KMIP server.

2.1 Authentication Suite

Implementations conformant to this profile SHALL support at least one of the Authentication Suites defined within [KMIP-PROF]. The establishment of the trust relationship between the KMIP client and the KMIP server is the same as the defined base profiles for the version of the profile supported.

2.2 Storage Array with Self-Encrypting Drives

KMIP clients conformant to this profile:

1. SHALL conform to the KMIP Baseline Client profile in [KMIP-PROF] and [KMIP-SPEC]
2. SHOULD NOT use a *Custom Attribute* [KMIP-SPEC] that duplicates information that is already in standard *Attributes* [KMIP-SPEC]

KMIP servers conformant to this profile SHALL:

1. SHALL conform to the KMIP Baseline Server profile in [KMIP-PROF] and [KMIP-SPEC] and
2. SHALL support the following *Objects* [KMIP-SPEC]
 - a. *Template* [KMIP-SPEC]
 - b. *Secret Data* [KMIP-SPEC]
3. SHALL support the following *Attributes* [KMIP-SPEC]
 - a. *Custom Attribute* [KMIP SPEC]
4. SHALL support the following client-to-server operations:
 - a. *Register* [KMIP-SPEC]
5. SHALL support the following *Message Encoding* [KMIP-SPEC]:
 - a. *Secret Data Type Enumeration* [KMIP-SPEC] value:
 - i. Password
 - b. *Object Type Enumeration* [KMIP-SPEC] values:
 - i. Secret Data
 - ii. Template
 - c. *Name Type Enumeration* [KMIP-SPEC] value:
 - i. Uninterpreted Text String
6. SHALL support *Custom Attribute* [KMIP-SPEC] with the following data types and properties:
 - a. TextString
7. SHALL support a minimum length of 64 characters for *Custom Attribute* [KMIP-SPEC] and *Name* [KMIP-SPEC] values where the attribute type is of variable length.
8. SHALL support a minimum of 10 *Custom Attribute* [KMIP-SPEC] per managed object
9. SHALL support a minimum of 64 characters in *Custom Attribute* [KMIP-SPEC] names
10. SHALL support the Storage Array with Self-Encrypting Drives Test Cases returning results in accordance with the test cases.
11. MAY support any clause within [KMIP-SPEC] provided it does not conflict with any other clause within this section 2.2

103 12. MAY support extensions outside the scope of this standard (e.g., vendor extensions,
104 conformance clauses) that do not contradict any KMIP requirements.

3 Storage Array with Self-Encrypting Drives Test Cases

This section documents the test cases that a client or server conformant to the Storage Array with Self-Encrypting Drives Profile SHALL support.

Note: the values for the returned items and the custom attributes are illustrative. Actual values from a real client system will vary. These test cases demonstrate usage of all of the mandatory types that are required to be supported in a server implementation.

3.1 Mandatory Test Cases

This section documents the test cases that a client or server conformant to the Storage Array with Self-Encrypting Drives Profile SHALL support for each version of the KMIP protocol (major and minor).

3.1.1 SASSED-M-1-10 - Configuration

Determine server configuration details including operations supported (only the mandatory operations are listed in the response example), objects supported (only the mandatory objects types are listed in the response example), and optional server information.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Query"/>
0011	<RequestPayload>
0012	<QueryFunction type="Enumeration" value="QueryOperations"/>
0013	<QueryFunction type="Enumeration" value="QueryObjects"/>
0014	<QueryFunction type="Enumeration"
	value="QueryServerInformation"/>
0015	</RequestPayload>
0016	</BatchItem>
0017	</RequestMessage>
0018	<ResponseMessage>
0019	<ResponseHeader>
0020	<ProtocolVersion>
0021	<ProtocolVersionMajor type="Integer" value="1"/>
0022	<ProtocolVersionMinor type="Integer" value="0"/>
0023	</ProtocolVersion>
0024	<TimeStamp type="DateTime" value="2013-04-25T16:53:03+00:00"/>
0025	<BatchCount type="Integer" value="1"/>
0026	</ResponseHeader>
0027	<BatchItem>
0028	<Operation type="Enumeration" value="Query"/>
0029	<ResultStatus type="Enumeration" value="Success"/>
0030	<ResponsePayload>
0031	<Operation type="Enumeration" value="Query"/>
0032	<Operation type="Enumeration" value="Locate"/>

0033	<Operation type="Enumeration" value="Destroy"/>
0034	<Operation type="Enumeration" value="Get"/>
0035	<Operation type="Enumeration" value="Register"/>
0036	<Operation type="Enumeration" value="GetAttributes"/>
0037	<Operation type="Enumeration" value="GetAttributeList"/>
0038	<Operation type="Enumeration" value="AddAttribute"/>
0039	<ObjectType type="Enumeration" value="SecretData"/>
0040	<ObjectType type="Enumeration" value="Template"/>
0041	<VendorIdentification type="TextString" value="server-
	vendor.com"/>
0042	<ServerInformation>
0043	</ServerInformation>
0044	</ResponsePayload>
0045	</BatchItem>
0046	</ResponseMessage>

119

120 3.1.2 SASSED-M-2-10 - Register the authentication key

121 A template is created and the secret data for the authentication key is then registered. The server must
 122 allow the registration of managed objects for Object Groups either by allowed arbitrary values for Object
 123 Groups or by pre-configuration of specific Object Groups prior to the storage array registering the
 124 authentication key. The authentication key may be a new authentication key or a replacement
 125 authentication key.

126

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="0"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Locate"/>
0011	<RequestPayload>
0012	<Attribute>
0013	<AttributeName type="TextString" value="Name"/>
0014	<AttributeValue>
0015	<NameValue type="TextString" value="SASED-M-2-10-
	templatel"/>
0016	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0017	</AttributeValue>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Object Type"/>
0021	<AttributeValue type="Enumeration" value="Template"/>
0022	</Attribute>
0023	</RequestPayload>
0024	</BatchItem>
0025	</RequestMessage>
0026	<ResponseMessage>
0027	<ResponseHeader>
0028	<ProtocolVersion>
0029	<ProtocolVersionMajor type="Integer" value="1"/>

0030	<ProtocolVersionMinor type="Integer" value="0"/>
0031	</ProtocolVersion>
0032	<TimeStamp type="DateTime" value="2013-04-25T16:53:08+00:00"/>
0033	<BatchCount type="Integer" value="1"/>
0034	</ResponseHeader>
0035	<BatchItem>
0036	<Operation type="Enumeration" value="Locate"/>
0037	<ResultStatus type="Enumeration" value="Success"/>
0038	<ResponsePayload>
0039	</ResponsePayload>
0040	</BatchItem>
0041	</ResponseMessage>
# TIME 1	
0042	<RequestMessage>
0043	<RequestHeader>
0044	<ProtocolVersion>
0045	<ProtocolVersionMajor type="Integer" value="1"/>
0046	<ProtocolVersionMinor type="Integer" value="0"/>
0047	</ProtocolVersion>
0048	<BatchCount type="Integer" value="1"/>
0049	</RequestHeader>
0050	<BatchItem>
0051	<Operation type="Enumeration" value="Register"/>
0052	<RequestPayload>
0053	<ObjectType type="Enumeration" value="Template"/>
0054	<TemplateAttribute>
0055	</TemplateAttribute>
0056	<Template>
0057	<Attribute>
0058	<AttributeName type="TextString" value="Object Group"/>
0059	<AttributeValue type="TextString" value="SASED-M-2-10-
0060	group"/>
0061	</Attribute>
0062	<Attribute>
0063	<AttributeName type="TextString" value="x-
0064	CustomAttribute1"/>
0065	<AttributeValue type="TextString" value="CustomValue1"/>
0066	</Attribute>
0067	<Attribute>
0068	<AttributeName type="TextString" value="x-
0069	CustomAttribute2"/>
0070	<AttributeValue type="TextString" value="CustomValue2"/>
0071	</Attribute>
0072	<Attribute>
0073	<AttributeName type="TextString" value="Name"/>
0074	<AttributeValue type="TextString" value="SASED-M-2-10-
0075	templatel"/>
0076	<NameType type="Enumeration"
0077	value="UninterpretedTextString"/>
0078	</AttributeValue>
0079	</Attribute>
0080	</Template>
0081	</RequestPayload>
0082	</BatchItem>
0083	</RequestMessage>
0084	<ResponseMessage>
0085	<ResponseHeader>

0082	<ProtocolVersion>
0083	<ProtocolVersionMajor type="Integer" value="1"/>
0084	<ProtocolVersionMinor type="Integer" value="0"/>
0085	</ProtocolVersion>
0086	<TimeStamp type="DateTime" value="2013-04-25T16:53:08+00:00"/>
0087	<BatchCount type="Integer" value="1"/>
0088	</ResponseHeader>
0089	<BatchItem>
0090	<Operation type="Enumeration" value="Register"/>
0091	<ResultStatus type="Enumeration" value="Success"/>
0092	<ResponsePayload>
0093	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0094	</ResponsePayload>
0095	</BatchItem>
0096	</ResponseMessage>
	# TIME 2
0097	<RequestMessage>
0098	<RequestHeader>
0099	<ProtocolVersion>
0100	<ProtocolVersionMajor type="Integer" value="1"/>
0101	<ProtocolVersionMinor type="Integer" value="0"/>
0102	</ProtocolVersion>
0103	<BatchCount type="Integer" value="1"/>
0104	</RequestHeader>
0105	<BatchItem>
0106	<Operation type="Enumeration" value="Register"/>
0107	<RequestPayload>
0108	<ObjectType type="Enumeration" value="SecretData"/>
0109	<TemplateAttribute>
0110	<Name>
0111	<NameValue type="TextString" value="SASED-M-2-10-
	template1"/>
0112	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0113	</Name>
0114	<Attribute>
0115	<AttributeName type="TextString" value="x-
	CustomAttribute3"/>
0116	<AttributeValue type="TextString" value="CustomValue3"/>
0117	</Attribute>
0118	<Attribute>
0119	<AttributeName type="TextString" value="x-
	CustomAttribute4"/>
0120	<AttributeValue type="TextString" value="CustomValue4"/>
0121	</Attribute>
0122	<Attribute>
0123	<AttributeName type="TextString" value="Name"/>
0124	<AttributeValue>
0125	<NameValue type="TextString" value="SASED-M-2-10-name"/>
0126	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0127	</AttributeValue>
0128	</Attribute>
0129	</TemplateAttribute>
0130	<SecretData>
0131	<SecretDataType type="Enumeration" value="Password"/>
0132	<KeyBlock>

[illegible]

127

128 3.1.3 SASSED-M-3-10 - Retrieve Authentication Key

129 Locate and retrieve the previously registered authentication key and finally destroy both the
130 authentication key and the template.

```

0001 # TIME 0
0002 <RequestMessage>
0003   <RequestHeader>
0004     <ProtocolVersion>
0005       <ProtocolVersionMajor type="Integer" value="1"/>
0006       <ProtocolVersionMinor type="Integer" value="0"/>
0007     </ProtocolVersion>
0008     <BatchCount type="Integer" value="1"/>
0009   </RequestHeader>
0010   <BatchItem>
0011     <Operation type="Enumeration" value="Locate"/>
0012   <RequestPayload>
0013     <Attribute>
0014       <AttributeName type="TextString" value="Object Group"/>
0015       <AttributeValue type="TextString" value="SASED-M-2-10-
group"/>
0016     </Attribute>
0017     <Attribute>
0018       <AttributeName type="TextString" value="Object Type"/>
0019       <AttributeValue type="Enumeration" value="SecretData"/>
0020     </Attribute>
0021   </RequestPayload>

```

0021	</BatchItem>
0022	</RequestMessage>
0023	<ResponseMessage>
0024	<ResponseHeader>
0025	<ProtocolVersion>
0026	<ProtocolVersionMajor type="Integer" value="1"/>
0027	<ProtocolVersionMinor type="Integer" value="0"/>
0028	</ProtocolVersion>
0029	<TimeStamp type="DateTime" value="2013-04-25T16:53:13+00:00"/>
0030	<BatchCount type="Integer" value="1"/>
0031	</ResponseHeader>
0032	<BatchItem>
0033	<Operation type="Enumeration" value="Locate"/>
0034	<ResultStatus type="Enumeration" value="Success"/>
0035	<ResponsePayload>
0036	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0037	</ResponsePayload>
0038	</BatchItem>
0039	</ResponseMessage>
# TIME 1	
0040	<RequestMessage>
0041	<RequestHeader>
0042	<ProtocolVersion>
0043	<ProtocolVersionMajor type="Integer" value="1"/>
0044	<ProtocolVersionMinor type="Integer" value="0"/>
0045	</ProtocolVersion>
0046	<BatchCount type="Integer" value="1"/>
0047	</RequestHeader>
0048	<BatchItem>
0049	<Operation type="Enumeration" value="GetAttributes"/>
0050	<RequestPayload>
0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	<AttributeName type="TextString" value="x-CustomAttribute4"/>
0053	</RequestPayload>
0054	</BatchItem>
0055	</RequestMessage>
0056	<ResponseMessage>
0057	<ResponseHeader>
0058	<ProtocolVersion>
0059	<ProtocolVersionMajor type="Integer" value="1"/>
0060	<ProtocolVersionMinor type="Integer" value="0"/>
0061	</ProtocolVersion>
0062	<TimeStamp type="DateTime" value="2013-04-25T16:53:14+00:00"/>
0063	<BatchCount type="Integer" value="1"/>
0064	</ResponseHeader>
0065	<BatchItem>
0066	<Operation type="Enumeration" value="GetAttributes"/>
0067	<ResultStatus type="Enumeration" value="Success"/>
0068	<ResponsePayload>
0069	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0070	<Attribute>
0071	<AttributeName type="TextString" value="x-
	CustomAttribute4"/>
0072	<AttributeValue type="TextString" value="CustomValue4"/>
0073	</Attribute>

0074	</ResponsePayload>
0075	</BatchItem>
0076	</ResponseMessage>
0077	# TIME 2
0078	<RequestMessage>
0079	<RequestHeader>
0080	<ProtocolVersion>
0081	<ProtocolVersionMajor type="Integer" value="1"/>
0082	<ProtocolVersionMinor type="Integer" value="0"/>
0083	</ProtocolVersion>
0084	<BatchCount type="Integer" value="1"/>
0085	</RequestHeader>
0086	<BatchItem>
0087	<Operation type="Enumeration" value="GetAttributes"/>
0088	<RequestPayload>
0089	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0090	<AttributeName type="TextString" value="x-CustomAttribute3"/>
0091	</RequestPayload>
0092	</BatchItem>
0093	</RequestMessage>
0094	<ResponseMessage>
0095	<ResponseHeader>
0096	<ProtocolVersion>
0097	<ProtocolVersionMajor type="Integer" value="1"/>
0098	<ProtocolVersionMinor type="Integer" value="0"/>
0099	</ProtocolVersion>
0100	<TimeStamp type="DateTime" value="2013-04-25T16:53:14+00:00"/>
0101	<BatchCount type="Integer" value="1"/>
0102	</ResponseHeader>
0103	<BatchItem>
0104	<Operation type="Enumeration" value="GetAttributes"/>
0105	<ResultStatus type="Enumeration" value="Success"/>
0106	<ResponsePayload>
0107	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>
0108	<Attribute>
0109	<AttributeName type="TextString" value="x-CustomAttribute3"/>
0110	<AttributeValue type="TextString" value="CustomValue3"/>
0111	</Attribute>
0112	</ResponsePayload>
0113	</BatchItem>
0114	</ResponseMessage>
0115	# TIME 3
0116	<RequestMessage>
0117	<RequestHeader>
0118	<ProtocolVersion>
0119	<ProtocolVersionMajor type="Integer" value="1"/>
0120	<ProtocolVersionMinor type="Integer" value="0"/>
0121	</ProtocolVersion>
0122	<BatchCount type="Integer" value="1"/>
0123	</RequestHeader>
0124	<BatchItem>
0125	<Operation type="Enumeration" value="Get"/>
0126	<RequestPayload>
0127	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_0"/>

0179	</ResponseHeader>
0180	<BatchItem>
0181	<Operation type="Enumeration" value="Destroy"/>
0182	<ResultStatus type="Enumeration" value="Success"/>
0183	<ResponsePayload>
0184	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0185	</ResponsePayload>
0186	</BatchItem>
0187	</ResponseMessage>
# TIME 5	
0188	<RequestMessage>
0189	<RequestHeader>
0190	<ProtocolVersion>
0191	<ProtocolVersionMajor type="Integer" value="1"/>
0192	<ProtocolVersionMinor type="Integer" value="0"/>
0193	</ProtocolVersion>
0194	<BatchCount type="Integer" value="1"/>
0195	</RequestHeader>
0196	<BatchItem>
0197	<Operation type="Enumeration" value="Locate"/>
0198	<RequestPayload>
0199	<Attribute>
0200	<AttributeName type="TextString" value="Name"/>
0201	<AttributeValue>
0202	<NameValue type="TextString" value="SASED-M-2-10-
	templatel"/>
0203	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0204	</AttributeValue>
0205	</Attribute>
0206	<Attribute>
0207	<AttributeName type="TextString" value="Object Type"/>
0208	<AttributeValue type="Enumeration" value="Template"/>
0209	</Attribute>
0210	</RequestPayload>
0211	</BatchItem>
0212	</RequestMessage>
0213	<ResponseMessage>
0214	<ResponseHeader>
0215	<ProtocolVersion>
0216	<ProtocolVersionMajor type="Integer" value="1"/>
0217	<ProtocolVersionMinor type="Integer" value="0"/>
0218	</ProtocolVersion>
0219	<TimeStamp type="DateTime" value="2013-04-25T16:53:08+00:00"/>
0220	<BatchCount type="Integer" value="1"/>
0221	</ResponseHeader>
0222	<BatchItem>
0223	<Operation type="Enumeration" value="Locate"/>
0224	<ResultStatus type="Enumeration" value="Success"/>
0225	<ResponsePayload>
0226	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0227	</ResponsePayload>
0228	</BatchItem>
0229	</ResponseMessage>
# TIME 6	
0230	<RequestMessage>

0231	<RequestHeader>
0232	<ProtocolVersion>
0233	<ProtocolVersionMajor type="Integer" value="1"/>
0234	<ProtocolVersionMinor type="Integer" value="0"/>
0235	</ProtocolVersion>
0236	<BatchCount type="Integer" value="1"/>
0237	</RequestHeader>
0238	<BatchItem>
0239	<Operation type="Enumeration" value="Destroy"/>
0240	<RequestPayload>
0241	<UniqueIdentifier type="TextString"
0242	value="\$UNIQUE_IDENTIFIER_1"/>
0243	</RequestPayload>
0244	</BatchItem>
0245	</RequestMessage>
0245	<ResponseMessage>
0246	<ResponseHeader>
0247	<ProtocolVersion>
0248	<ProtocolVersionMajor type="Integer" value="1"/>
0249	<ProtocolVersionMinor type="Integer" value="0"/>
0250	</ProtocolVersion>
0251	<TimeStamp type="DateTime" value="2013-04-25T17:01:41+00:00"/>
0252	<BatchCount type="Integer" value="1"/>
0253	</ResponseHeader>
0254	<BatchItem>
0255	<Operation type="Enumeration" value="Destroy"/>
0256	<ResultStatus type="Enumeration" value="Success"/>
0257	<ResponsePayload>
0258	<UniqueIdentifier type="TextString"
0259	value="\$UNIQUE_IDENTIFIER_1"/>
0260	</ResponsePayload>
0261	</BatchItem>
0261	</ResponseMessage>

131

132 3.1.4 SASSED-M-1-11 - Configuration

133 Determine server configuration details including operations supported (only the mandatory operations are
134 listed in the response example), objects supported (only the mandatory objects types are listed in the
135 response example), and optional server information.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Query"/>
0011	<RequestPayload>
0012	<QueryFunction type="Enumeration" value="QueryOperations"/>
0013	<QueryFunction type="Enumeration" value="QueryObjects"/>
0014	<QueryFunction type="Enumeration"
0015	value="QueryServerInformation"/>
0015	</RequestPayload>

0016	</BatchItem>
0017	</RequestMessage>
0018	<ResponseMessage>
0019	<ResponseHeader>
0020	<ProtocolVersion>
0021	<ProtocolVersionMajor type="Integer" value="1"/>
0022	<ProtocolVersionMinor type="Integer" value="1"/>
0023	</ProtocolVersion>
0024	<TimeStamp type="DateTime" value="2013-04-25T16:53:03+00:00"/>
0025	<BatchCount type="Integer" value="1"/>
0026	</ResponseHeader>
0027	<BatchItem>
0028	<Operation type="Enumeration" value="Query"/>
0029	<ResultStatus type="Enumeration" value="Success"/>
0030	<ResponsePayload>
0031	<Operation type="Enumeration" value="Query"/>
0032	<Operation type="Enumeration" value="Locate"/>
0033	<Operation type="Enumeration" value="Destroy"/>
0034	<Operation type="Enumeration" value="Get"/>
0035	<Operation type="Enumeration" value="Register"/>
0036	<Operation type="Enumeration" value="GetAttributes"/>
0037	<Operation type="Enumeration" value="GetAttributeList"/>
0038	<Operation type="Enumeration" value="AddAttribute"/>
0039	<ObjectType type="Enumeration" value="SecretData"/>
0040	<ObjectType type="Enumeration" value="Template"/>
0041	<VendorIdentification type="TextString" value="server- vendor.com"/>
0042	<ServerInformation>
0043	</ServerInformation>
0044	</ResponsePayload>
0045	</BatchItem>
0046	</ResponseMessage>

136

137 3.1.5 SASSED-M-2-11 - Register the authentication key

138 A template is created and the secret data for the authentication key is then registered. The server must
139 allow the registration of managed objects for Object Groups either by allowed arbitrary values for Object
140 Groups or by pre-configuration of specific Object Groups prior to the storage array registering the
141 authentication key. The authentication key may be a new authentication key or a replacement
142 authentication key.

143

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Locate"/>
0011	<RequestPayload>
0012	<Attribute>
0013	<AttributeName type="TextString" value="Name"/>
0014	<AttributeValue>

0015	<NameValue type="TextString" value="SASED-M-2-11-templatel"/>
0016	<NameType type="Enumeration" value="UninterpretedTextString"/>
0017	</AttributeValue>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Object Type"/>
0021	<AttributeValue type="Enumeration" value="Template"/>
0022	</Attribute>
0023	</RequestPayload>
0024	</BatchItem>
0025	</RequestMessage>
0026	<ResponseMessage>
0027	<ResponseHeader>
0028	<ProtocolVersion>
0029	<ProtocolVersionMajor type="Integer" value="1"/>
0030	<ProtocolVersionMinor type="Integer" value="1"/>
0031	</ProtocolVersion>
0032	<TimeStamp type="DateTime" value="2013-04-25T16:53:08+00:00"/>
0033	<BatchCount type="Integer" value="1"/>
0034	</ResponseHeader>
0035	<BatchItem>
0036	<Operation type="Enumeration" value="Locate"/>
0037	<ResultStatus type="Enumeration" value="Success"/>
0038	<ResponsePayload>
0039	</ResponsePayload>
0040	</BatchItem>
0041	</ResponseMessage>
# TIME 1	
0042	<RequestMessage>
0043	<RequestHeader>
0044	<ProtocolVersion>
0045	<ProtocolVersionMajor type="Integer" value="1"/>
0046	<ProtocolVersionMinor type="Integer" value="1"/>
0047	</ProtocolVersion>
0048	<BatchCount type="Integer" value="1"/>
0049	</RequestHeader>
0050	<BatchItem>
0051	<Operation type="Enumeration" value="Register"/>
0052	<RequestPayload>
0053	<ObjectType type="Enumeration" value="Template"/>
0054	<TemplateAttribute>
0055	</TemplateAttribute>
0056	<Template>
0057	<Attribute>
0058	<AttributeName type="TextString" value="Object Group"/>
0059	<AttributeValue type="TextString" value="SASED-M-2-11-group"/>
0060	</Attribute>
0061	<Attribute>
0062	<AttributeName type="TextString" value="x-CustomAttribute1"/>
0063	<AttributeValue type="TextString" value="CustomValue1"/>
0064	</Attribute>
0065	<Attribute>
0066	<AttributeName type="TextString" value="x-CustomAttribute2"/>

0067	<AttributeValue type="TextString" value="CustomValue2"/>
0068	</Attribute>
0069	<Attribute>
0070	<AttributeName type="TextString" value="Name"/>
0071	<AttributeValue>
0072	<NameValue type="TextString" value="SASED-M-2-11-
	template1"/>
0073	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0074	</AttributeValue>
0075	</Attribute>
0076	</Template>
0077	</RequestPayload>
0078	</BatchItem>
0079	</RequestMessage>
0080	<ResponseMessage>
0081	<ResponseHeader>
0082	<ProtocolVersion>
0083	<ProtocolVersionMajor type="Integer" value="1"/>
0084	<ProtocolVersionMinor type="Integer" value="1"/>
0085	</ProtocolVersion>
0086	<TimeStamp type="DateTime" value="2013-04-25T16:53:08+00:00"/>
0087	<BatchCount type="Integer" value="1"/>
0088	</ResponseHeader>
0089	<BatchItem>
0090	<Operation type="Enumeration" value="Register"/>
0091	<ResultStatus type="Enumeration" value="Success"/>
0092	<ResponsePayload>
0093	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0094	</ResponsePayload>
0095	</BatchItem>
0096	</ResponseMessage>
	# TIME 2
0097	<RequestMessage>
0098	<RequestHeader>
0099	<ProtocolVersion>
0100	<ProtocolVersionMajor type="Integer" value="1"/>
0101	<ProtocolVersionMinor type="Integer" value="1"/>
0102	</ProtocolVersion>
0103	<BatchCount type="Integer" value="1"/>
0104	</RequestHeader>
0105	<BatchItem>
0106	<Operation type="Enumeration" value="Register"/>
0107	<RequestPayload>
0108	<ObjectType type="Enumeration" value="SecretData"/>
0109	<TemplateAttribute>
0110	<Name>
0111	<NameValue type="TextString" value="SASED-M-2-11-
	template1"/>
0112	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0113	</Name>
0114	<Attribute>
0115	<AttributeName type="TextString" value="x-
	CustomAttribute3"/>
0116	<AttributeValue type="TextString" value="CustomValue3"/>
0117	</Attribute>

0005	<ProtocolVersionMinor type="Integer" value="1"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Locate"/>
0011	<RequestPayload>
0012	<Attribute>
0013	<AttributeName type="TextString" value="Object Group"/>
0014	<AttributeValue type="TextString" value="SASED-M-2-11-
	group"/>
0015	</Attribute>
0016	<Attribute>
0017	<AttributeName type="TextString" value="Object Type"/>
0018	<AttributeValue type="Enumeration" value="SecretData"/>
0019	</Attribute>
0020	</RequestPayload>
0021	</BatchItem>
0022	</RequestMessage>
0023	<ResponseMessage>
0024	<ResponseHeader>
0025	<ProtocolVersion>
0026	<ProtocolVersionMajor type="Integer" value="1"/>
0027	<ProtocolVersionMinor type="Integer" value="1"/>
0028	</ProtocolVersion>
0029	<TimeStamp type="DateTime" value="2013-04-25T16:53:13+00:00"/>
0030	<BatchCount type="Integer" value="1"/>
0031	</ResponseHeader>
0032	<BatchItem>
0033	<Operation type="Enumeration" value="Locate"/>
0034	<ResultStatus type="Enumeration" value="Success"/>
0035	<ResponsePayload>
0036	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER 0"/>
0037	</ResponsePayload>
0038	</BatchItem>
0039	</ResponseMessage>
	# TIME 1
0040	<RequestMessage>
0041	<RequestHeader>
0042	<ProtocolVersion>
0043	<ProtocolVersionMajor type="Integer" value="1"/>
0044	<ProtocolVersionMinor type="Integer" value="1"/>
0045	</ProtocolVersion>
0046	<BatchCount type="Integer" value="1"/>
0047	</RequestHeader>
0048	<BatchItem>
0049	<Operation type="Enumeration" value="GetAttributes"/>
0050	<RequestPayload>
0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	<AttributeName type="TextString" value="x-CustomAttribute4"/>
0053	</RequestPayload>
0054	</BatchItem>
0055	</RequestMessage>
0056	<ResponseMessage>
0057	<ResponseHeader>
0058	<ProtocolVersion>

0059	<ProtocolVersionMajor type="Integer" value="1"/>
0060	<ProtocolVersionMinor type="Integer" value="1"/>
0061	</ProtocolVersion>
0062	<TimeStamp type="DateTime" value="2013-04-25T16:53:14+00:00"/>
0063	<BatchCount type="Integer" value="1"/>
0064	</ResponseHeader>
0065	<BatchItem>
0066	<Operation type="Enumeration" value="GetAttributes"/>
0067	<ResultStatus type="Enumeration" value="Success"/>
0068	<ResponsePayload>
0069	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0070	<Attribute>
0071	<AttributeName type="TextString" value="x-
	CustomAttribute4"/>
0072	<AttributeValue type="TextString" value="CustomValue4"/>
0073	</Attribute>
0074	</ResponsePayload>
0075	</BatchItem>
0076	</ResponseMessage>
# TIME 2	
0077	<RequestMessage>
0078	<RequestHeader>
0079	<ProtocolVersion>
0080	<ProtocolVersionMajor type="Integer" value="1"/>
0081	<ProtocolVersionMinor type="Integer" value="1"/>
0082	</ProtocolVersion>
0083	<BatchCount type="Integer" value="1"/>
0084	</RequestHeader>
0085	<BatchItem>
0086	<Operation type="Enumeration" value="GetAttributes"/>
0087	<RequestPayload>
0088	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0089	<AttributeName type="TextString" value="x-CustomAttribute3"/>
0090	</RequestPayload>
0091	</BatchItem>
0092	</RequestMessage>
0093	<ResponseMessage>
0094	<ResponseHeader>
0095	<ProtocolVersion>
0096	<ProtocolVersionMajor type="Integer" value="1"/>
0097	<ProtocolVersionMinor type="Integer" value="1"/>
0098	</ProtocolVersion>
0099	<TimeStamp type="DateTime" value="2013-04-25T16:53:14+00:00"/>
0100	<BatchCount type="Integer" value="1"/>
0101	</ResponseHeader>
0102	<BatchItem>
0103	<Operation type="Enumeration" value="GetAttributes"/>
0104	<ResultStatus type="Enumeration" value="Success"/>
0105	<ResponsePayload>
0106	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0107	<Attribute>
0108	<AttributeName type="TextString" value="x-
	CustomAttribute3"/>
0109	<AttributeValue type="TextString" value="CustomValue3"/>
0110	</Attribute>

0163	</RequestHeader>
0164	<BatchItem>
0165	<Operation type="Enumeration" value="Destroy"/>
0166	<RequestPayload>
0167	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0168	</RequestPayload>
0169	</BatchItem>
0170	</RequestMessage>
0171	<ResponseMessage>
0172	<ResponseHeader>
0173	<ProtocolVersion>
0174	<ProtocolVersionMajor type="Integer" value="1"/>
0175	<ProtocolVersionMinor type="Integer" value="1"/>
0176	</ProtocolVersion>
0177	<TimeStamp type="DateTime" value="2013-04-25T17:01:41+00:00"/>
0178	<BatchCount type="Integer" value="1"/>
0179	</ResponseHeader>
0180	<BatchItem>
0181	<Operation type="Enumeration" value="Destroy"/>
0182	<ResultStatus type="Enumeration" value="Success"/>
0183	<ResponsePayload>
0184	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0185	</ResponsePayload>
0186	</BatchItem>
0187	</ResponseMessage>
	# TIME 5
0188	<RequestMessage>
0189	<RequestHeader>
0190	<ProtocolVersion>
0191	<ProtocolVersionMajor type="Integer" value="1"/>
0192	<ProtocolVersionMinor type="Integer" value="1"/>
0193	</ProtocolVersion>
0194	<BatchCount type="Integer" value="1"/>
0195	</RequestHeader>
0196	<BatchItem>
0197	<Operation type="Enumeration" value="Locate"/>
0198	<RequestPayload>
0199	<Attribute>
0200	<AttributeName type="TextString" value="Name"/>
0201	<AttributeValue>
0202	<NameValue type="TextString" value="SASED-M-2-11-
	template1"/>
0203	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0204	</AttributeValue>
0205	</Attribute>
0206	<Attribute>
0207	<AttributeName type="TextString" value="Object Type"/>
0208	<AttributeValue type="Enumeration" value="Template"/>
0209	</Attribute>
0210	</RequestPayload>
0211	</BatchItem>
0212	</RequestMessage>
0213	<ResponseMessage>
0214	<ResponseHeader>
0215	<ProtocolVersion>

0216	<ProtocolVersionMajor type="Integer" value="1"/>
0217	<ProtocolVersionMinor type="Integer" value="1"/>
0218	</ProtocolVersion>
0219	<TimeStamp type="DateTime" value="2013-04-25T16:53:08+00:00"/>
0220	<BatchCount type="Integer" value="1"/>
0221	</ResponseHeader>
0222	<BatchItem>
0223	<Operation type="Enumeration" value="Locate"/>
0224	<ResultStatus type="Enumeration" value="Success"/>
0225	<ResponsePayload>
0226	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0227	</ResponsePayload>
0228	</BatchItem>
0229	</ResponseMessage>
# TIME 6	
0230	<RequestMessage>
0231	<RequestHeader>
0232	<ProtocolVersion>
0233	<ProtocolVersionMajor type="Integer" value="1"/>
0234	<ProtocolVersionMinor type="Integer" value="1"/>
0235	</ProtocolVersion>
0236	<BatchCount type="Integer" value="1"/>
0237	</RequestHeader>
0238	<BatchItem>
0239	<Operation type="Enumeration" value="Destroy"/>
0240	<RequestPayload>
0241	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0242	</RequestPayload>
0243	</BatchItem>
0244	</RequestMessage>
0245	<ResponseMessage>
0246	<ResponseHeader>
0247	<ProtocolVersion>
0248	<ProtocolVersionMajor type="Integer" value="1"/>
0249	<ProtocolVersionMinor type="Integer" value="1"/>
0250	</ProtocolVersion>
0251	<TimeStamp type="DateTime" value="2013-04-25T17:01:41+00:00"/>
0252	<BatchCount type="Integer" value="1"/>
0253	</ResponseHeader>
0254	<BatchItem>
0255	<Operation type="Enumeration" value="Destroy"/>
0256	<ResultStatus type="Enumeration" value="Success"/>
0257	<ResponsePayload>
0258	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0259	</ResponsePayload>
0260	</BatchItem>
0261	</ResponseMessage>

148

149 3.1.7 SASSED-M-1-12 - Configuration

150 Determine server configuration details including operations supported (only the mandatory operations are
151 listed in the response example), objects supported (only the mandatory objects types are listed in the
152 response example), and optional server information.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Query"/>
0011	<RequestPayload>
0012	<QueryFunction type="Enumeration" value="QueryOperations"/>
0013	<QueryFunction type="Enumeration" value="QueryObjects"/>
0014	<QueryFunction type="Enumeration"
	value="QueryServerInformation"/>
0015	</RequestPayload>
0016	</BatchItem>
0017	</RequestMessage>
0018	<ResponseMessage>
0019	<ResponseHeader>
0020	<ProtocolVersion>
0021	<ProtocolVersionMajor type="Integer" value="1"/>
0022	<ProtocolVersionMinor type="Integer" value="2"/>
0023	</ProtocolVersion>
0024	<TimeStamp type="DateTime" value="2013-04-25T16:53:03+00:00"/>
0025	<BatchCount type="Integer" value="1"/>
0026	</ResponseHeader>
0027	<BatchItem>
0028	<Operation type="Enumeration" value="Query"/>
0029	<ResultStatus type="Enumeration" value="Success"/>
0030	<ResponsePayload>
0031	<Operation type="Enumeration" value="Query"/>
0032	<Operation type="Enumeration" value="Locate"/>
0033	<Operation type="Enumeration" value="Destroy"/>
0034	<Operation type="Enumeration" value="Get"/>
0035	<Operation type="Enumeration" value="Register"/>
0036	<Operation type="Enumeration" value="GetAttributes"/>
0037	<Operation type="Enumeration" value="GetAttributeList"/>
0038	<Operation type="Enumeration" value="AddAttribute"/>
0039	<ObjectType type="Enumeration" value="SecretData"/>
0040	<ObjectType type="Enumeration" value="Template"/>
0041	<VendorIdentification type="TextString" value="server-
	vendor.com"/>
0042	<ServerInformation>
0043	</ServerInformation>
0044	</ResponsePayload>
0045	</BatchItem>
0046	</ResponseMessage>

153

154 3.1.8 SASSED-M-2-12 - Register the authentication key

155 A template is created and the secret data for the authentication key is then registered. The server must
156 allow the registration of managed objects for Object Groups either by allowed arbitrary values for Object
157 Groups or by pre-configuration of specific Object Groups prior to the storage array registering the

158 authentication key. The authentication key may be a new authentication key or a replacement
 159 authentication key.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Locate"/>
0011	<RequestPayload>
0012	<Attribute>
0013	<AttributeName type="TextString" value="Name"/>
0014	<AttributeValue>
0015	<NameValue type="TextString" value="SASED-M-2-12-
	templatel"/>
0016	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0017	</AttributeValue>
0018	</Attribute>
0019	<Attribute>
0020	<AttributeName type="TextString" value="Object Type"/>
0021	<AttributeValue type="Enumeration" value="Template"/>
0022	</Attribute>
0023	</RequestPayload>
0024	</BatchItem>
0025	</RequestMessage>
0026	<ResponseMessage>
0027	<ResponseHeader>
0028	<ProtocolVersion>
0029	<ProtocolVersionMajor type="Integer" value="1"/>
0030	<ProtocolVersionMinor type="Integer" value="2"/>
0031	</ProtocolVersion>
0032	<TimeStamp type="DateTime" value="2013-04-25T16:53:08+00:00"/>
0033	<BatchCount type="Integer" value="1"/>
0034	</ResponseHeader>
0035	<BatchItem>
0036	<Operation type="Enumeration" value="Locate"/>
0037	<ResultStatus type="Enumeration" value="Success"/>
0038	<ResponsePayload>
0039	</ResponsePayload>
0040	</BatchItem>
0041	</ResponseMessage>
	# TIME 1
0042	<RequestMessage>
0043	<RequestHeader>
0044	<ProtocolVersion>
0045	<ProtocolVersionMajor type="Integer" value="1"/>
0046	<ProtocolVersionMinor type="Integer" value="2"/>
0047	</ProtocolVersion>
0048	<BatchCount type="Integer" value="1"/>
0049	</RequestHeader>
0050	<BatchItem>
0051	<Operation type="Enumeration" value="Register"/>

0052	<RequestPayload>
0053	<ObjectType type="Enumeration" value="Template"/>
0054	<TemplateAttribute>
0055	<Attribute>
0056	<AttributeName type="TextString" value="Name"/>
0057	<AttributeValue>
0058	<NameValue type="TextString" value="SASED-M-2-12-
	templatel"/>
0059	<NameType type="Enumeration"
	value="UninterpretedTextString"/>
0060	</AttributeValue>
0061	</Attribute>
0062	</TemplateAttribute>
0063	<Template>
0064	<Attribute>
0065	<AttributeName type="TextString" value="Object Group"/>
0066	<AttributeValue type="TextString" value="SASED-M-2-12-
	group"/>
0067	</Attribute>
0068	<Attribute>
0069	<AttributeName type="TextString" value="x-
	CustomAttribute1"/>
0070	<AttributeValue type="TextString" value="CustomValue1"/>
0071	</Attribute>
0072	<Attribute>
0073	<AttributeName type="TextString" value="x-
	CustomAttribute2"/>
0074	<AttributeValue type="TextString" value="CustomValue2"/>
0075	</Attribute>
0076	</Template>
0077	</RequestPayload>
0078	</BatchItem>
0079	</RequestMessage>
0080	<ResponseMessage>
0081	<ResponseHeader>
0082	<ProtocolVersion>
0083	<ProtocolVersionMajor type="Integer" value="1"/>
0084	<ProtocolVersionMinor type="Integer" value="2"/>
0085	</ProtocolVersion>
0086	<TimeStamp type="DateTime" value="2013-04-25T16:53:08+00:00"/>
0087	<BatchCount type="Integer" value="1"/>
0088	</ResponseHeader>
0089	<BatchItem>
0090	<Operation type="Enumeration" value="Register"/>
0091	<ResultStatus type="Enumeration" value="Success"/>
0092	<ResponsePayload>
0093	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0094	</ResponsePayload>
0095	</BatchItem>
0096	</ResponseMessage>
	# TIME 2
0097	<RequestMessage>
0098	<RequestHeader>
0099	<ProtocolVersion>
0100	<ProtocolVersionMajor type="Integer" value="1"/>
0101	<ProtocolVersionMinor type="Integer" value="2"/>
0102	</ProtocolVersion>

0154	<ResponsePayload>
0155	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0156	</ResponsePayload>
0157	</BatchItem>
0158	</ResponseMessage>

160

161 3.1.9 SASSED-M-3-12 - Retrieve Authentication Key

162 Locate and retrieve the previously registered authentication key and finally destroy both the
163 authentication key and the template.

	# TIME 0
0001	<RequestMessage>
0002	<RequestHeader>
0003	<ProtocolVersion>
0004	<ProtocolVersionMajor type="Integer" value="1"/>
0005	<ProtocolVersionMinor type="Integer" value="2"/>
0006	</ProtocolVersion>
0007	<BatchCount type="Integer" value="1"/>
0008	</RequestHeader>
0009	<BatchItem>
0010	<Operation type="Enumeration" value="Locate"/>
0011	<RequestPayload>
0012	<Attribute>
0013	<AttributeName type="TextString" value="Object Group"/>
0014	<AttributeValue type="TextString" value="SASSED-M-2-12-
	group"/>
0015	</Attribute>
0016	<Attribute>
0017	<AttributeName type="TextString" value="Object Type"/>
0018	<AttributeValue type="Enumeration" value="SecretData"/>
0019	</Attribute>
0020	</RequestPayload>
0021	</BatchItem>
0022	</RequestMessage>
0023	<ResponseMessage>
0024	<ResponseHeader>
0025	<ProtocolVersion>
0026	<ProtocolVersionMajor type="Integer" value="1"/>
0027	<ProtocolVersionMinor type="Integer" value="2"/>
0028	</ProtocolVersion>
0029	<TimeStamp type="DateTime" value="2013-04-25T16:53:13+00:00"/>
0030	<BatchCount type="Integer" value="1"/>
0031	</ResponseHeader>
0032	<BatchItem>
0033	<Operation type="Enumeration" value="Locate"/>
0034	<ResultStatus type="Enumeration" value="Success"/>
0035	<ResponsePayload>
0036	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0037	</ResponsePayload>
0038	</BatchItem>
0039	</ResponseMessage>
	# TIME 1
0040	<RequestMessage>
0041	<RequestHeader>

0042	<ProtocolVersion>
0043	<ProtocolVersionMajor type="Integer" value="1"/>
0044	<ProtocolVersionMinor type="Integer" value="2"/>
0045	</ProtocolVersion>
0046	<BatchCount type="Integer" value="1"/>
0047	</RequestHeader>
0048	<BatchItem>
0049	<Operation type="Enumeration" value="GetAttributes"/>
0050	<RequestPayload>
0051	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0052	<AttributeName type="TextString" value="x-CustomAttribute4"/>
0053	</RequestPayload>
0054	</BatchItem>
0055	</RequestMessage>
0056	<ResponseMessage>
0057	<ResponseHeader>
0058	<ProtocolVersion>
0059	<ProtocolVersionMajor type="Integer" value="1"/>
0060	<ProtocolVersionMinor type="Integer" value="2"/>
0061	</ProtocolVersion>
0062	<TimeStamp type="DateTime" value="2013-04-25T16:53:14+00:00"/>
0063	<BatchCount type="Integer" value="1"/>
0064	</ResponseHeader>
0065	<BatchItem>
0066	<Operation type="Enumeration" value="GetAttributes"/>
0067	<ResultStatus type="Enumeration" value="Success"/>
0068	<ResponsePayload>
0069	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0070	<Attribute>
0071	<AttributeName type="TextString" value="x-
	CustomAttribute4"/>
0072	<AttributeValue type="TextString" value="CustomValue4"/>
0073	</Attribute>
0074	</ResponsePayload>
0075	</BatchItem>
0076	</ResponseMessage>
	# TIME 2
0077	<RequestMessage>
0078	<RequestHeader>
0079	<ProtocolVersion>
0080	<ProtocolVersionMajor type="Integer" value="1"/>
0081	<ProtocolVersionMinor type="Integer" value="2"/>
0082	</ProtocolVersion>
0083	<BatchCount type="Integer" value="1"/>
0084	</RequestHeader>
0085	<BatchItem>
0086	<Operation type="Enumeration" value="GetAttributes"/>
0087	<RequestPayload>
0088	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0089	<AttributeName type="TextString" value="x-CustomAttribute3"/>
0090	</RequestPayload>
0091	</BatchItem>
0092	</RequestMessage>
0093	<ResponseMessage>
0094	<ResponseHeader>

0095	<ProtocolVersion>
0096	<ProtocolVersionMajor type="Integer" value="1"/>
0097	<ProtocolVersionMinor type="Integer" value="2"/>
0098	</ProtocolVersion>
0099	<TimeStamp type="DateTime" value="2013-04-25T16:53:14+00:00"/>
0100	<BatchCount type="Integer" value="1"/>
0101	</ResponseHeader>
0102	<BatchItem>
0103	<Operation type="Enumeration" value="GetAttributes"/>
0104	<ResultStatus type="Enumeration" value="Success"/>
0105	<ResponsePayload>
0106	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0107	<Attribute>
0108	<AttributeName type="TextString" value="x-
	CustomAttribute3"/>
0109	<AttributeValue type="TextString" value="CustomValue3"/>
0110	</Attribute>
0111	</ResponsePayload>
0112	</BatchItem>
0113	</ResponseMessage>
# TIME 3	
0114	<RequestMessage>
0115	<RequestHeader>
0116	<ProtocolVersion>
0117	<ProtocolVersionMajor type="Integer" value="1"/>
0118	<ProtocolVersionMinor type="Integer" value="2"/>
0119	</ProtocolVersion>
0120	<BatchCount type="Integer" value="1"/>
0121	</RequestHeader>
0122	<BatchItem>
0123	<Operation type="Enumeration" value="Get"/>
0124	<RequestPayload>
0125	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0126	</RequestPayload>
0127	</BatchItem>
0128	</RequestMessage>
0129	<ResponseMessage>
0130	<ResponseHeader>
0131	<ProtocolVersion>
0132	<ProtocolVersionMajor type="Integer" value="1"/>
0133	<ProtocolVersionMinor type="Integer" value="2"/>
0134	</ProtocolVersion>
0135	<TimeStamp type="DateTime" value="2013-04-25T17:01:41+00:00"/>
0136	<BatchCount type="Integer" value="1"/>
0137	</ResponseHeader>
0138	<BatchItem>
0139	<Operation type="Enumeration" value="Get"/>
0140	<ResultStatus type="Enumeration" value="Success"/>
0141	<ResponsePayload>
0142	<ObjectType type="Enumeration" value="SecretData"/>
0143	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_0"/>
0144	<SecretData>
0145	<SecretDataType type="Enumeration" value="Password"/>
0146	<KeyBlock>
0147	<KeyFormatType type="Enumeration" value="Opaque"/>

0200	<AttributeName type="TextString" value="Name"/>
0201	<AttributeValue>
0202	<NameValue type="TextString" value="SASED-M-2-12- templatel"/>
0203	<NameType type="Enumeration" value="UninterpretedTextString"/>
0204	</AttributeValue>
0205	</Attribute>
0206	<Attribute>
0207	<AttributeName type="TextString" value="Object Type"/>
0208	<AttributeValue type="Enumeration" value="Template"/>
0209	</Attribute>
0210	</RequestPayload>
0211	</BatchItem>
0212	</RequestMessage>
0213	<ResponseMessage>
0214	<ResponseHeader>
0215	<ProtocolVersion>
0216	<ProtocolVersionMajor type="Integer" value="1"/>
0217	<ProtocolVersionMinor type="Integer" value="2"/>
0218	</ProtocolVersion>
0219	<TimeStamp type="DateTime" value="2013-04-25T16:53:08+00:00"/>
0220	<BatchCount type="Integer" value="1"/>
0221	</ResponseHeader>
0222	<BatchItem>
0223	<Operation type="Enumeration" value="Locate"/>
0224	<ResultStatus type="Enumeration" value="Success"/>
0225	<ResponsePayload>
0226	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0227	</ResponsePayload>
0228	</BatchItem>
0229	</ResponseMessage>
0230	# TIME 6 <RequestMessage>
0231	<RequestHeader>
0232	<ProtocolVersion>
0233	<ProtocolVersionMajor type="Integer" value="1"/>
0234	<ProtocolVersionMinor type="Integer" value="2"/>
0235	</ProtocolVersion>
0236	<BatchCount type="Integer" value="1"/>
0237	</RequestHeader>
0238	<BatchItem>
0239	<Operation type="Enumeration" value="Destroy"/>
0240	<RequestPayload>
0241	<UniqueIdentifier type="TextString" value="\$UNIQUE_IDENTIFIER_1"/>
0242	</RequestPayload>
0243	</BatchItem>
0244	</RequestMessage>
0245	<ResponseMessage>
0246	<ResponseHeader>
0247	<ProtocolVersion>
0248	<ProtocolVersionMajor type="Integer" value="1"/>
0249	<ProtocolVersionMinor type="Integer" value="2"/>
0250	</ProtocolVersion>
0251	<TimeStamp type="DateTime" value="2013-04-25T17:01:41+00:00"/>
0252	<BatchCount type="Integer" value="1"/>

0253	</ResponseHeader>
0254	<BatchItem>
0255	<Operation type="Enumeration" value="Destroy"/>
0256	<ResultStatus type="Enumeration" value="Success"/>
0257	<ResponsePayload>
0258	<UniqueIdentifier type="TextString"
	value="\$UNIQUE_IDENTIFIER_1"/>
0259	</ResponsePayload>
0260	</BatchItem>
0261	</ResponseMessage>

164

165

4 Conformance

4.1 Conformance Statement

KMIP client and server implementations conformant to this profile:

1. SHALL support the Authentication Suite conditions (2.1)
2. SHALL support the Storage Array with Self-Encrypting Drives conditions (2.2)
3. SHALL support all the Mandatory Test Cases (3.1) for each supported protocol version (major and minor)

4.2 Permitted Test Case Variations

Whilst the test cases provided in this Profile define the allowed request and response content, some inherent variations MAY occur and are permitted within a successfully completed test case.

Each test case MAY include allowed variations in the description of the test case in addition to the variations noted in this section.

Other variations not explicitly noted in this Profile SHALL be deemed non-conformant.

4.2.1 Variable Items

An implementation conformant to this Profile MAY vary the following values:

1. UniqueIdentifier
2. PrivateKeyUniqueIdentifier
3. PublicKeyUniqueIdentifier
4. UniqueBatchItemIdentifier
5. AsynchronousCorrelationValue
6. TimeStamp
7. KeyValue / KeyMaterial including:
 - a. key material content returned for managed cryptographic objects which are generated by the server
 - b. wrapped versions of keys where the wrapping key is dynamic or the wrapping contains variable output for each wrap operation
8. For response containing the output of cryptographic operation in Data / SignatureData/ MACData / IVCounterNonce where:
 - a. the managed object is generated by the server; or
 - b. the operation inherently contains variable output
9. For the following DateTime attributes where the value is not specified in the request as a fixed DateTime value:
 - a. ActivationDate
 - b. ArchiveDate
 - c. CompromiseDate
 - d. CompromiseOccurrenceDate
 - e. DeactivationDate
 - f. DestroyDate
 - g. InitialDate

- 205 h. LastChangeDate
- 206 i. ProtectStartDate
- 207 j. ProcessStopDate
- 208 k. ValidityDate
- 209 l. OriginalCreationDate
- 210 10. LinkedObjectIdentifier
- 211 11. DigestValue
 - 212 a. For those managed cryptographic objects which are dynamically generated
- 213 12. KeyFormatType
 - 214 a. The key format type selected by the server when it creates managed objects
- 215 13. Digest
 - 216 a. The HashingAlgorithm selected by the server when it calculates the digest for a managed
 - 217 object for which it has access to the key material
 - 218 b. The Digest Value
- 219 14. Extensions reported in Query for ExtensionList and ExtensionMap
- 220 15. Application Namespaces reported in Query
- 221 16. Object Types reported in Query other than those noted as required in this profile
- 222 17. Operation Types reported in Query other than those noted as required in this profile (or any
- 223 referenced profile documents)
- 224 18. For TextString attribute values containing test identifiers:
 - 225 a. Additional vendor or application prefixes
- 226 19. Additional attributes beyond those noted in the response

227

228 An implementation conformant to this Profile MAY allow the following response variations:

- 229 1. Object Group values – May or may not return one or more Object Group values not included in
- 230 the requests
- 231 2. y-CustomAttributes – May or may not include additional server-specific associated attributes not
- 232 included in requests
- 233 3. Message Extensions – May or may not include additional (non-critical) vendor extensions
- 234 4. TemplateAttribute – May or may not be included in responses where the Template Attribute
- 235 response is noted as optional in [KMIP-SPEC]
- 236 5. AttributeIndex – May or may not include Attribute Index value where the Attribute Index value is 0
- 237 for Protocol Versions 1.1 and above.
- 238 6. ResultMessage – May or may not be included in responses and the value (if included) may vary
- 239 from the text contained within the test case.
- 240 7. The list of Protocol Versions returned in a DiscoverVersion response may include additional
- 241 protocol versions if the request has not specified a list of client supported Protocol Versions.
- 242 8. VendorIdentification - The value (if included) may vary from the text contained within the test
- 243 case.

244 4.2.2 Variable behavior

245 An implementation conformant to this Profile SHALL allow variation of the following behavior:

- 246 1. A test may omit the clean-up requests and responses (containing Revoke and/or Destroy) at the
- 247 end of the test provided there is a separate mechanism to remove the created objects during
- 248 testing.

249 2. A test may omit the test identifiers if the client is unable to include them in requests. This includes
250 the following attributes:
251 a. Name; and
252 b. x-ID
253
254

Appendix A. Acknowledgments

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

Participants:

255 Hal Aldridge, Sypris Electronics
256 Mike Allen, Symantec
257 Gordon Arnold, IBM
258 Todd Arnold, IBM
259 Richard Austin, Hewlett-Packard
260 Lars Bagnert, PrimeKey
261 Elaine Barker, NIST
262 Peter Bartok, Venafi, Inc.
263 Tom Benjamin, IBM
264 Anthony Berglas, Cryptsoft
265 Mathias Björkqvist, IBM
266 Kevin Bocket, Venafi
267 Anne Bolgert, IBM
268 Alan Brown, Thales e-Security
269 Tim Bruce, CA Technologies
270 Chris Burchett, Credant Technologies, Inc.
271 Kelley Burgin, National Security Agency
272 Robert Burns, Thales e-Security
273 Chuck Castleton, Venafi
274 Kenli Chong, QuintessenceLabs
275 John Clark, Hewlett-Packard
276 Tom Clifford, Symantec Corp.
277 Doron Cohen, SafeNet, Inc
278 Tony Cox, Cryptsoft
279 Russell Dietz, SafeNet, Inc
280 Graydon Dodson, Lexmark International Inc.
281 Vinod Duggirala, EMC Corporation
282 Chris Dunn, SafeNet, Inc.
283 Michael Duren, Sypris Electronics
284 James Dzierzanowski, American Express CCoE
285 Faisal Faruqui, Thales e-Security
286 Stan Feather, Hewlett-Packard
287 David Finkelstein, Symantec Corp.
288 James Fitzgerald, SafeNet, Inc.
289 Indra Fitzgerald, Hewlett-Packard
290 Judith Furlong, EMC Corporation
291 Susan Gleeson, Oracle
292 Robert Griffin, EMC Corporation
293 Paul Grojean, Individual
294 Robert Haas, IBM
295 Thomas Hardjono, M.I.T.
296 ChengDong He, Huawei Technologies Co., Ltd.
297 Steve He, Vormetric
298 Kurt Heberlein, Hewlett-Packard
299 Larry Hofer, Emulex Corporation
300 Maryann Hondo, IBM
301 Walt Hubis, NetApp
302 Tim Hudson, Cryptsoft
303 Jonas Iggbom, Venafi, Inc.

304 Sitaram Inguva, American Express CCoE
 305 Jay Jacobs, Target Corporation
 306 Glen Jaquette, IBM
 307 Mahadev Karadiguddi, NetApp
 308 Greg Kazmierczak, Wave Systems Corp.
 309 Marc Kenig, SafeNet, Inc.
 310 Mark Knight, Thales e-Security
 311 Kathy Kriese, Symantec Corporation
 312 Mark Lambiase, SecureAuth
 313 John Leiseboer, Quintessence Labs
 314 Hal Lockhart, Oracle Corporation
 315 Robert Lockhart, Thales e-Security
 316 Anne Luk, Cryptsoft
 317 Sairam Manidi, Freescale
 318 Luther Martin, Voltage Security
 319 Neil McEvoy, iFOSSF
 320 Marina Milshtein, Individual
 321 Dale Moberg, Axway Software
 322 Jishnu Mukeri, Hewlett-Packard
 323 Bryan Olson, Hewlett-Packard
 324 John Peck, IBM
 325 Rob Philpott, EMC Corporation
 326 Denis Pochuev, SafeNet, Inc.
 327 Reid Poole, Venafi, Inc.
 328 Ajai Puri, SafeNet, Inc.
 329 Saravanan Ramalingam, Thales e-Security
 330 Peter Reed, SafeNet, Inc.
 331 Bruce Rich, IBM
 332 Christina Richards, American Express CCoE
 333 Warren Robbins, Dell
 334 Peter Robinson, EMC Corporation
 335 Scott Rotondo, Oracle
 336 Saikat Saha, SafeNet, Inc.
 337 Anil Saldhana, Red Hat
 338 Subhash Sankuratiripati, NetApp
 339 Boris Schumperli, Cryptomathic
 340 Greg Singh, QuintessenceLabs
 341 David Smith, Venafi, Inc.
 342 Brian Spector, Certivox
 343 Terence Spies, Voltage Security
 344 Deborah Steckroth, RouteOne LLC
 345 Michael Stevens, QuintessenceLabs
 346 Marcus Streets, Thales e-Security
 347 Satish Sundar, IBM
 348 Kiran Thota, VMware
 349 Somanchi Trinath, Freescale Semiconductor, Inc.
 350 Nathan Turajski, Thales e-Security
 351 Sean Turner, IECA, Inc.
 352 Paul Turner, Venafi, Inc.
 353 Rod Wideman, Quantum Corporation
 354 Steven Wierenga, Hewlett-Packard
 355 Jin Wong, QuintessenceLabs
 356 Sameer Yami, Thales e-Security
 357 Peter Yee, EMC Corporation
 358 Krishna Yellepeddy, IBM
 359 Catherine Ying, SafeNet, Inc.
 360 Tatu Ylonen, SSH Communications Security (Tectia Corp)

361 Michael Yoder, Vormetric. Inc.
362 Magda Zdunkiewicz, Cryptsoft
363 Peter Zelechowski, Election Systems & Software

Appendix B. KMIP Specification Cross Reference

Reference Term	KMIP 1.0	KMIP 1.1	KMIP 1.2
1 Introduction			
<i>Non-Normative References</i>	1.3.	1.3.	1.3.
<i>Normative References</i>	1.2.	1.2.	1.2.
<i>Terminology</i>	1.1.	1.1.	1.1.
2 Objects			
<i>Attribute</i>	2.1.1.	2.1.1.	2.1.1.
<i>Base Objects</i>	2.1.	2.1.	2.1.
<i>Certificate</i>	2.2.1.	2.2.1.	2.2.1.
<i>Credential</i>	2.1.2.	2.1.2.	2.1.2.
<i>Data</i>	-	-	2.1.10.
<i>Data Length</i>	-	-	2.1.11.
<i>Extension Information</i>	-	2.1.9.	2.1.9.
<i>Key Block</i>	2.1.3.	2.1.3.	2.1.3.
<i>Key Value</i>	2.1.4.	2.1.4.	2.1.4.
<i>Key Wrapping Data</i>	2.1.5.	2.1.5.	2.1.5.
<i>Key Wrapping Specification</i>	2.1.6.	2.1.6.	2.1.6.
<i>MAC Data</i>	-	-	2.1.13.
<i>Managed Objects</i>	2.2.	2.2.	2.2.
<i>Nonce</i>	-	-	2.1.14.
<i>Opaque Object</i>	2.2.8.	2.2.8.	2.2.8.
<i>PGP Key</i>	-	-	2.2.9.
<i>Private Key</i>	2.2.4.	2.2.4.	2.2.4.
<i>Public Key</i>	2.2.3.	2.2.3.	2.2.3.
<i>Secret Data</i>	2.2.7.	2.2.7.	2.2.7.
<i>Signature Data</i>	-	-	2.1.12.
<i>Split Key</i>	2.2.5.	2.2.5.	2.2.5.
<i>Symmetric Key</i>	2.2.2.	2.2.2.	2.2.2.
<i>Template</i>	2.2.6.	2.2.6.	2.2.6.
<i>Template-Attribute Structures</i>	2.1.8.	2.1.8.	2.1.8.
<i>Transparent DH Private Key</i>	2.1.7.6.	2.1.7.6.	2.1.7.6.
<i>Transparent DH Public Key</i>	2.1.7.7.	2.1.7.7.	2.1.7.7.
<i>Transparent DSA Private Key</i>	2.1.7.2.	2.1.7.2.	2.1.7.2.
<i>Transparent DSA Public Key</i>	2.1.7.3.	2.1.7.3.	2.1.7.3.
<i>Transparent ECDH Private Key</i>	2.1.7.10.	2.1.7.10.	2.1.7.10.
<i>Transparent ECDH Public Key</i>	2.1.7.11.	2.1.7.11.	2.1.7.11.
<i>Transparent ECDSA Private Key</i>	2.1.7.8.	2.1.7.8.	2.1.7.8.
<i>Transparent ECDSA Public Key</i>	2.1.7.9.	2.1.7.9.	2.1.7.9.
<i>Transparent ECMQV Private Key</i>	2.1.7.12.	2.1.7.12.	2.1.7.12.
<i>Transparent ECMQV Public Key</i>	2.1.7.13.	2.1.7.13.	2.1.7.13.
<i>Transparent Key Structures</i>	2.1.7.	2.1.7.	2.1.7.
<i>Transparent RSA Private Key</i>	2.1.7.4.	2.1.7.4.	2.1.7.4.
<i>Transparent RSA Public Key</i>	2.1.7.5.	2.1.7.5.	2.1.7.5.
<i>Transparent Symmetric Key</i>	2.1.7.1.	2.1.7.1.	2.1.7.1.
3 Attributes			
<i>Activation Date</i>	3.19.	3.24.	3.24.
<i>Alternative Name</i>	-	-	3.40.
<i>Application Specific Information</i>	3.30.	3.36.	3.36.
<i>Archive Date</i>	3.27.	3.32.	3.32.

Reference Term	KMIP 1.0	KMIP 1.1	KMIP 1.2
<i>Attributes</i>	3	3	3
<i>Certificate Identifier</i>	3.9.	3.13.	3.13.
<i>Certificate Issuer</i>	3.11.	3.15.	3.15.
<i>Certificate Length</i>	-	3.9.	3.9.
<i>Certificate Subject</i>	3.10.	3.14.	3.14.
<i>Certificate Type</i>	3.8.	3.8.	3.8.
<i>Compromise Date</i>	3.25.	3.30.	3.30.
<i>Compromise Occurrence Date</i>	3.24.	3.29.	3.29.
<i>Contact Information</i>	3.31.	3.37.	3.37.
<i>Cryptographic Algorithm</i>	3.4.	3.4.	3.4.
<i>Cryptographic Domain Parameters</i>	3.7.	3.7.	3.7.
<i>Cryptographic Length</i>	3.5.	3.5.	3.5.
<i>Cryptographic Parameters</i>	3.6.	3.6.	3.6.
<i>Custom Attribute</i>	3.33.	3.39.	3.39.
<i>Deactivation Date</i>	3.22.	3.27.	3.27.
<i>Default Operation Policy</i>	3.13.2.	3.18.2.	3.18.2.
<i>Default Operation Policy for Certificates and Public Key Objects</i>	3.13.2.2.	3.18.2.2.	3.18.2.2.
<i>Default Operation Policy for Secret Objects</i>	3.13.2.1.	3.18.2.1.	3.18.2.1.
<i>Default Operation Policy for Template Objects</i>	3.13.2.3.	3.18.2.3.	3.18.2.3.
<i>Destroy Date</i>	3.23.	3.28.	3.28.
<i>Digest</i>	3.12.	3.17.	3.17.
<i>Digital Signature Algorithm</i>	-	3.16.	3.16.
<i>Fresh</i>	-	3.34.	3.34.
<i>Initial Date</i>	3.18.	3.23.	3.23.
<i>Key Value Location</i>	-	-	3.42.
<i>Key Value Present</i>	-	-	3.41.
<i>Last Change Date</i>	3.32.	3.38.	3.38.
<i>Lease Time</i>	3.15.	3.20.	3.20.
<i>Link</i>	3.29.	3.35.	3.35.
<i>Name</i>	3.2.	3.2.	3.2.
<i>Object Group</i>	3.28.	3.33.	3.33.
<i>Object Type</i>	3.3.	3.3.	3.3.
<i>Operation Policy Name</i>	3.13.	3.18.	3.18.
<i>Operations outside of operation policy control</i>	3.13.1.	3.18.1.	3.18.1.
<i>Original Creation Date</i>	-	-	3.43.
<i>Process Start Date</i>	3.20.	3.25.	3.25.
<i>Protect Stop Date</i>	3.21.	3.26.	3.26.
<i>Revocation Reason</i>	3.26.	3.31.	3.31.
<i>State</i>	3.17.	3.22.	3.22.
<i>Unique Identifier</i>	3.1.	3.1.	3.1.
<i>Usage Limits</i>	3.16.	3.21.	3.21.
<i>X.509 Certificate Identifier</i>	-	3.10.	3.10.
<i>X.509 Certificate Issuer</i>	-	3.12.	3.12.
<i>X.509 Certificate Subject</i>	-	3.11.	3.11.
4 Client-to-Server Operations			
<i>Activate</i>	4.18.	4.19.	4.19.
<i>Add Attribute</i>	4.13.	4.14.	4.14.
<i>Archive</i>	4.21.	4.22.	4.22.
<i>Cancel</i>	4.25.	4.27.	4.27.
<i>Certify</i>	4.6.	4.7.	4.7.
<i>Check</i>	4.9.	4.10.	4.10.
<i>Create</i>	4.1.	4.1.	4.1.
<i>Create Key Pair</i>	4.2.	4.2.	4.2.

Reference Term	KMIP 1.0	KMIP 1.1	KMIP 1.2
<i>Create Split Key</i>	-	-	4.38.
<i>Decrypt</i>	-	-	4.30.
<i>Delete Attribute</i>	4.15.	4.16.	4.16.
<i>Derive Key</i>	4.5.	4.6.	4.6.
<i>Destroy</i>	4.20.	4.21.	4.21.
<i>Discover Versions</i>	-	4.26.	4.26.
<i>Encrypt</i>	-	-	4.29.
<i>Get</i>	4.10.	4.11.	4.11.
<i>Get Attribute List</i>	4.12.	4.13.	4.13.
<i>Get Attributes</i>	4.11.	4.12.	4.12.
<i>Get Usage Allocation</i>	4.17.	4.18.	4.18.
<i>Hash</i>	-	-	4.37.
<i>Join Split Key</i>	-	-	4.39.
<i>Locate</i>	4.8.	4.9.	4.9.
<i>MAC</i>	-	-	4.33.
<i>MAC Verify</i>	-	-	4.34.
<i>Modify Attribute</i>	4.14.	4.15.	4.15.
<i>Obtain Lease</i>	4.16.	4.17.	4.17.
<i>Poll</i>	4.26.	4.28.	4.28.
<i>Query</i>	4.24.	4.25.	4.25.
<i>Re-certify</i>	4.7.	4.8.	4.8.
<i>Recover</i>	4.22.	4.23.	4.23.
<i>Register</i>	4.3.	4.3.	4.3.
<i>Re-key</i>	4.4.	4.4.	4.4.
<i>Re-key Key Pair</i>	-	4.5.	4.5.
<i>Revoke</i>	4.19.	4.20.	4.20.
<i>RNG Retrieve</i>	-	-	4.35.
<i>RNG Seed</i>	-	-	4.36.
<i>Sign</i>	-	-	4.31.
<i>Signature Verify</i>	-	-	4.32.
<i>Validate</i>	4.23.	4.24.	4.24.
5 Server-to-Client Operations			
<i>Notify</i>	5.1.	5.1.	5.1.
<i>Put</i>	5.2.	5.2.	5.2.
6 Message Contents			
<i>Asynchronous Correlation Value</i>	6.8.	6.8.	6.8.
<i>Asynchronous Indicator</i>	6.7.	6.7.	6.7.
<i>Attestation Capable Indicator</i>	-	-	6.17.
<i>Batch Count</i>	6.14.	6.14.	6.14.
<i>Batch Error Continuation Option</i>	6.13.	6.13.	6.13.
<i>Batch Item</i>	6.15.	6.15.	6.15.
<i>Batch Order Option</i>	6.12.	6.12.	6.12.
<i>Maximum Response Size</i>	6.3.	6.3.	6.3.
<i>Message Extension</i>	6.16.	6.16.	6.16.
<i>Operation</i>	6.2.	6.2.	6.2.
<i>Protocol Version</i>	6.1.	6.1.	6.1.
<i>Result Message</i>	6.11.	6.11.	6.11.
<i>Result Reason</i>	6.10.	6.10.	6.10.
<i>Result Status</i>	6.9.	6.9.	6.9.
<i>Time Stamp</i>	6.5.	6.5.	6.5.
<i>Unique Batch Item ID</i>	6.4.	6.4.	6.4.
7 Message Format			

Reference Term	KMIP 1.0	KMIP 1.1	KMIP 1.2
<i>Message Structure</i>	7.1.	7.1.	7.1.
<i>Operations</i>	7.2.	7.2.	7.2.
8 Authentication			
<i>Authentication</i>	8	8	8
9 Message Encoding			
<i>Alternative Name Type Enumeration</i>	-	-	9.1.3.2.34.
<i>Attestation Type Enumeration</i>	-	-	9.1.3.2.36.
<i>Batch Error Continuation Option Enumeration</i>	9.1.3.2.29.	9.1.3.2.30.	9.1.3.2.30.
<i>Bit Masks</i>	9.1.3.3.	9.1.3.3.	9.1.3.3.
<i>Block Cipher Mode Enumeration</i>	9.1.3.2.13.	9.1.3.2.14.	9.1.3.2.14.
<i>Cancellation Result Enumeration</i>	9.1.3.2.24.	9.1.3.2.25.	9.1.3.2.25.
<i>Certificate Request Type Enumeration</i>	9.1.3.2.21.	9.1.3.2.22.	9.1.3.2.22.
<i>Certificate Type Enumeration</i>	9.1.3.2.6.	9.1.3.2.6.	9.1.3.2.6.
<i>Credential Type Enumeration</i>	9.1.3.2.1.	9.1.3.2.1.	9.1.3.2.1.
<i>Cryptographic Algorithm Enumeration</i>	9.1.3.2.12.	9.1.3.2.13.	9.1.3.2.13.
<i>Cryptographic Usage Mask</i>	9.1.3.3.1.	9.1.3.3.1.	9.1.3.3.1.
<i>Defined Values</i>	9.1.3.	9.1.3.	9.1.3.
<i>Derivation Method Enumeration</i>	9.1.3.2.20.	9.1.3.2.21.	9.1.3.2.21.
<i>Digital Signature Algorithm Enumeration</i>	-	9.1.3.2.7.	9.1.3.2.7.
<i>Encoding Option Enumeration</i>	-	9.1.3.2.32.	9.1.3.2.32.
<i>Enumerations</i>	9.1.3.2.	9.1.3.2.	9.1.3.2.
<i>Examples</i>	9.1.2.	9.1.2.	9.1.2.
<i>Hashing Algorithm Enumeration</i>	9.1.3.2.15.	9.1.3.2.16.	9.1.3.2.16.
<i>Item Length</i>	9.1.1.3.	9.1.1.3.	9.1.1.3.
<i>Item Tag</i>	9.1.1.1.	9.1.1.1.	9.1.1.1.
<i>Item Type</i>	9.1.1.2.	9.1.1.2.	9.1.1.2.
<i>Item Value</i>	9.1.1.4.	9.1.1.4.	9.1.1.4.
<i>Key Compression Type Enumeration</i>	9.1.3.2.2.	9.1.3.2.2.	9.1.3.2.2.
<i>Key Format Type Enumeration</i>	9.1.3.2.3.	9.1.3.2.3.	9.1.3.2.3.
<i>Key Role Type Enumeration</i>	9.1.3.2.16.	9.1.3.2.17.	9.1.3.2.17.
<i>Key Value Location Type Enumeration</i>	-	-	9.1.3.2.35.
<i>Link Type Enumeration</i>	9.1.3.2.19.	9.1.3.2.20.	9.1.3.2.20.
<i>Name Type Enumeration</i>	9.1.3.2.10.	9.1.3.2.11.	9.1.3.2.11.
<i>Object Group Member Enumeration</i>	-	9.1.3.2.33.	9.1.3.2.33.
<i>Object Type Enumeration</i>	9.1.3.2.11.	9.1.3.2.12.	9.1.3.2.12.
<i>Opaque Data Type Enumeration</i>	9.1.3.2.9.	9.1.3.2.10.	9.1.3.2.10.
<i>Operation Enumeration</i>	9.1.3.2.26.	9.1.3.2.27.	9.1.3.2.27.
<i>Padding Method Enumeration</i>	9.1.3.2.14.	9.1.3.2.15.	9.1.3.2.15.
<i>Put Function Enumeration</i>	9.1.3.2.25.	9.1.3.2.26.	9.1.3.2.26.
<i>Query Function Enumeration</i>	9.1.3.2.23.	9.1.3.2.24.	9.1.3.2.24.
<i>Recommended Curve Enumeration for ECDSA, ECDH, and ECMQV</i>	9.1.3.2.5.	9.1.3.2.5.	9.1.3.2.5.
<i>Result Reason Enumeration</i>	9.1.3.2.28.	9.1.3.2.29.	9.1.3.2.29.
<i>Result Status Enumeration</i>	9.1.3.2.27.	9.1.3.2.28.	9.1.3.2.28.
<i>Revocation Reason Code Enumeration</i>	9.1.3.2.18.	9.1.3.2.19.	9.1.3.2.19.
<i>Secret Data Type Enumeration</i>	9.1.3.2.8.	9.1.3.2.9.	9.1.3.2.9.
<i>Split Key Method Enumeration</i>	9.1.3.2.7.	9.1.3.2.8.	9.1.3.2.8.
<i>State Enumeration</i>	9.1.3.2.17.	9.1.3.2.18.	9.1.3.2.18.
<i>Storage Status Mask</i>	9.1.3.3.2.	9.1.3.3.2.	9.1.3.3.2.
<i>Tags</i>	9.1.3.1.	9.1.3.1.	9.1.3.1.
<i>TTLV Encoding</i>	9.1.	9.1.	9.1.
<i>TTLV Encoding Fields</i>	9.1.1.	9.1.1.	9.1.1.
<i>Usage Limits Unit Enumeration</i>	9.1.3.2.30.	9.1.3.2.31.	9.1.3.2.31.

Reference Term	KMIP 1.0	KMIP 1.1	KMIP 1.2
<i>Validity Indicator Enumeration</i>	9.1.3.2.22.	9.1.3.2.23.	9.1.3.2.23.
<i>Wrapping Method Enumeration</i>	9.1.3.2.4.	9.1.3.2.4.	9.1.3.2.4.
<i>XML Encoding</i>	9.2.	-	-
10 Transport			
<i>Transport</i>	10	10	10
12 KMIP Server and Client Implementation Conformance			
<i>Conformance clauses for a KMIP Server</i>	12.1.	-	-
<i>KMIP Client Implementation Conformance</i>	-	12.2.	12.2.
<i>KMIP Server Implementation Conformance</i>	-	12.1.	12.1.

Appendix C. Revision History

Revision	Date	Editor	Changes Made
wd01	21-May-2013	Tim Hudson / Mahadev Karadigudda	Converted from draft proposal to OASIS template with minor rewording and inclusion of references to KMIP 1.2 documents
wd02	25-June-2013	Tim Hudson	Updated test cases and changed how multiple versions of the specification are referenced and added test cases for all versions.
wd03	6-August-2013	Tim Hudson	Updated to include Permitted Test Case Variations and updated Test Cases based on July 2013 Interop
wd04	10-August-2013	Tim Hudson	Updated Permitted Test Case Variations
wd04a	24-October-2013	Tim Hudson	Editorial update to include VendorIdentification in the list of allowed variations as per TC motion.