

KMIP Suite B 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-suite-b-profile/v1.0/csprd01/kmip-suite-b-profile-v1.0-csprd01.doc> (Authoritative)
<http://docs.oasis-open.org/kmip/kmip-suite-b-profile/v1.0/csprd01/kmip-suite-b-profile-v1.0-csprd01.html>
<http://docs.oasis-open.org/kmip/kmip-suite-b-profile/v1.0/csprd01/kmip-suite-b-profile-v1.0-csprd01.pdf>

Previous version:

N/A

Latest version:

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

Kelley Burgin (kwburgi@tycho.ncsc.mil), National Security Agency
Tim Hudson (tjh@cryptsoft.com), Cryptsoft

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 KMIP clients and KMIP servers using Suite B cryptography that has been approved by NIST for use by the U.S. Government and specified in NIST standards or recommendations.

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-suite-b-v1.0]

KMIP Suite B Profile Version 1.0. Edited by Kelley Burgin and Tim Hudson. 09 January 2014. OASIS Committee Specification Draft 01 / Public Review Draft 01. <http://docs.oasis-open.org/kmip/kmip-suite-b-profile/v1.0/csprd01/kmip-suite-b-profile-v1.0-csprd01.html>. Latest version: <http://docs.oasis-open.org/kmip/kmip-suite-b-profile/v1.0/kmip-suite-b-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	6
1.2	Normative References	6
1.3	Non-Normative References	6
2	Suite B minLOS_128 Profile.....	8
2.1	Authentication Suite.....	8
2.1.1	Protocols.....	8
2.1.2	Cipher Suites	8
2.1.3	Client Authenticity.....	8
2.1.4	Object Owner.....	8
2.1.5	KMIP Port Number	8
2.2	Suite B minLOS_128	8
3	Suite B minLOS_128 Test Cases.....	11
3.1	Mandatory Test Cases.....	11
4	Suite B minLOS_192 Profile.....	12
4.1	Authentication Suite.....	12
4.1.1	Protocols.....	12
4.1.2	Cipher Suites	12
4.1.3	Client Authenticity.....	12
4.1.4	Object Owner.....	12
4.1.5	KMIP Port Number	12
4.2	Suite B minLOS_192	12
5	Suite B minLOS_192 Test Cases.....	15
5.1	Mandatory Test Cases.....	15
6	Conformance	16
6.1	Suite B minLOS_128 Profile Conformance	16
6.2	Suite B minLOS_192 Profile Conformance	16
6.3	Permitted Test Case Variations	16
6.3.1	Variable Items.....	16
6.3.2	Variable behavior	18
Appendix A.	Acknowledgments	19
Appendix B.	KMIP Specification Cross Reference	22
Appendix C.	Revision History	27

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].

Suite B [SuiteB] requires that key establishment and signature algorithms be based upon Elliptic Curve Cryptography and that the encryption algorithm be AES [FIPS197]. Suite B includes:

Encryption	Advanced Encryption Standard (AES) (key sizes of 128 and 256 bits)
Digital Signature	Elliptic Curve Digital Signature Algorithm (ECDSA) (using the curves with 256-bit and 384-bit prime moduli)
Key Exchange	Elliptic Curve Diffie-Hellman (ECDH), (using the curves with 256-bit and 384-bit prime moduli)
Hashes	SHA-256 and SHA-384

Suite B provides for two levels of cryptographic security, namely a 128-bit minimum level of security (minLOS_128) and a 192-bit minimum level of security (minLOS_192). Each level defines a minimum strength that all cryptographic algorithms must provide. A KMIP product configured at a minimum level of security of 128 bits provides adequate protection for classified information up to the SECRET level. A KMIP product configured at a minimum level of security of 192 bits is required to protect classified information at the TOP SECRET level.

The Suite B non-signature primitives are divided into two columns as shown below.

	Column 1	Column 2
Encryption	AES-128	AES-256
Key Agreement	ECDH on P-256	ECDH on P-384
Hash for PRF/MAC	SHA-256	SHA-384

At the 128-bit minimum level of security, the non-signature primitives MUST either come exclusively from Column 1 or exclusively from Column 2.

At the 192-bit minimum level of security, the non-signature primitives MUST come exclusively from Column 2.

Digital signatures using ECDSA MUST be used for authentication. Following the direction of RFC 4754, ECDSA-256 represents an instantiation of the ECDSA algorithm using the P-256 curve and the SHA-256 hash function. ECDSA-384 represents an instantiation of the ECDSA algorithm using the P-384 curve and the SHA-384 hash function.

If configured at a minimum level of security of 128 bits, a KMIP product MUST use either ECDSA-256 or ECDSA-384 for authentication. It is allowable for one party to authenticate with ECDSA-256 and the other party to authenticate with ECDSA-384. This flexibility will allow interoperability between a KMIP client and server that have different sizes of ECDSA authentication keys. KMIP products configured at a minimum level of security of 128 bits MUST be able to verify ECDSA-256 signatures and SHOULD be able to verify

ECDSA-384 signatures. If configured at a minimum level of security of 192 bits, ECDSA-384 MUST be used by both the KMIP client and server for authentication. KMIP products configured at a minimum level of security of 192 bits MUST be able to verify ECDSA-384 signatures.

KMIP products, at both minimum levels of security, MUST each use an X.509 certificate that complies with the "Suite B Certificate and Certificate Revocation List (CRL) Profile" [RFC5759] and that contains an elliptic curve public key with the key usage bit set for digital signature.

1.1 Terminology

The key words "MUST", "SHALL", "SHOULD", and "MAY" in this document are to be interpreted as described in [RFC2119].

1.2 Normative References

- [CNSSP-15] N.S.A., "National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems", 1 October 2013, https://www.cnss.gov/Assets/pdf/CNSSP_No%2015_minorUpdate1_Oct12012.pdf.
- [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>.
- [RFC4754] D. Fu and J. Solinas, *IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*, IETF RFC 4754, Jan 2007, <http://www.ietf.org/rfc/rfc4754.txt>.
- [RFC5246] Dierks, T. and E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.2*, IETF RFC 5246, August 2008, <http://www.ietf.org/rfc/rfc5246.txt>.
- [RFC6460] M. Salter and R. Housley, *Suite B Profile for Transport Layer Security (TLS)*, IETF RFC 6460, January 2012, <http://www.ietf.org/rfc/rfc6460.txt>.
- [KMIP-SPEC]
[KMIP-SPEC-1_0] One or more of [KMIP-SPEC-1_0], [KMIP-SPEC-1_1], [KMIP-SPEC-1_2]
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, 1 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](http://docs.oasis-open.org/kmip/spec/v1.2/os/kmip-spec-v1.2-os.doc), Candidate OASIS Standard 01, DD MMM YYYY.
- [KMIP-PROF]
[KMIP-PROF-1_0] One or more of [KMIP-PROF-1_0], [KMIP-PROF-1_1], [KMIP-PROF-1_2]
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](http://docs.oasis-open.org/kmip/profiles/v1.2/os/kmip-profiles-v1.2-os.doc), Candidate OASIS Standard 01, DD MMM YYYY.

1.3 Non-Normative References

- [KMIP-UG]
[KMIP-UG-1_0] One or more of [KMIP-UG-1_0], [KMIP-UG-1_1], [KMIP-UG-1_2]
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.

78 **[KMIP-UG-1_1]** *Key Management Interoperability Protocol Usage Guide Version 1.1,*
79 <http://docs.oasis-open.org/kmip/ug/v1.1/kmip-ug-v1.1-cnd01.doc>,
80 Committee Note Draft, 1 December 2011.

81 **[KMIP-UG-1_2]** *Key Management Interoperability Protocol Usage Guide Version 1.2,*
82 [URL](#), Committee Note Draft, **DD MMM YYYY**.

83 **[KMIP-TC-1_1]** *Key Management Interoperability Protocol Test Cases Version 1.1,*
84 [http://docs.oasis-open.org/kmip/testcases/v1.1/cn01/kmip-testcases-v1.1-](http://docs.oasis-open.org/kmip/testcases/v1.1/cn01/kmip-testcases-v1.1-cn01.doc)
85 [cn01.doc](http://docs.oasis-open.org/kmip/testcases/v1.1/cn01/kmip-testcases-v1.1-cn01.doc), Committee Note 01, 27 July 2012.

86 **[KMIP-TC-1_2]** *Key Management Interoperability Protocol Test Cases Version 1.2,*
87 [URL](#), Committee Note Draft, **DD MMM YYYY**.

88 **[KMIP-UC]** *Key Management Interoperability Protocol Use Cases Version 1.0,*
89 [http://docs.oasis-open.org/kmip/usecases/v1.0/cs01/kmip-usecases-1.0-cs-](http://docs.oasis-open.org/kmip/usecases/v1.0/cs01/kmip-usecases-1.0-cs-01.doc)
90 [01.doc](http://docs.oasis-open.org/kmip/usecases/v1.0/cs01/kmip-usecases-1.0-cs-01.doc), Committee Specification, 15 June 2010.

91 **[SuiteB]** *Suite B Cryptography / Cryptographic Interoperability,*
92 http://www.nsa.gov/ia/programs/suiteb_cryptography/

2 Suite B minLOS_128 Profile

The Suite B minLOS_128 Profile describes a KMIP client interacting with a KMIP server as an information assurance product to provide a minimum level of security of 128 bits.
(http://www.nsa.gov/ia/programs/suiteb_cryptography/)

2.1 Authentication Suite

Implementations conformant to this profile SHALL use TLS to negotiate a mutually-authenticated connection.

2.1.1 Protocols

Conformant KMIP clients and servers SHALL support:

- TLS v1.2 [RFC5246]

2.1.2 Cipher Suites

Conformant KMIP servers SHALL support the following cipher suites:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

2.1.3 Client Authenticity

Conformant KMIP servers and clients SHALL handle client authenticity in accordance with section 3.2.3 of the TLS 1.2 Authentication Suite [KMIP-PROF].

2.1.4 Object Owner

Conformant KMIP servers and clients SHALL handle object owner in accordance with section 3.2.4 of the TLS 1.2 Authentication Suite [KMIP-PROF].

2.1.5 KMIP Port Number

Conformant KMIP servers and clients SHALL handle the KMIP port number in accordance with section 3.2.5 of the TLS 1.2 Authentication Suite [KMIP-PROF].

2.2 Suite B minLOS_128

KMIP clients conformant to this profile under [KMIP-SPEC]:

1. SHALL conform to the Baseline Client conformance clauses in [KMIP-PROF] and [KMIP-SPEC]
2. SHALL restrict use of the enumerated types listed in item 6 of the server list below to the values noted against each item
3. MAY support any clause within [KMIP-SPEC] provided it does not conflict with any other clause within this section 2.2.
4. MAY support extensions outside the scope of this standard (e.g., vendor extensions, conformance clauses) that do not conflict with any KMIP or [CNSSP-15] requirements.

KMIP servers conformant to this profile under [KMIP-SPEC]:

1. SHALL conform to the Baseline Server profile in [KMIP-PROF] and [KMIP-SPEC] and
2. SHALL support the following *Objects* [KMIP-SPEC]
 - a. *Certificate* [KMIP-SPEC]

- b. *Symmetric Key* [KMIP-SPEC]
- c. *Public Key* [KMIP-SPEC]
- d. *Private Key* [KMIP-SPEC]
- 3. SHALL support the following *Attributes* [KMIP-SPEC]
 - a. *Cryptographic Algorithm* [KMIP-SPEC]
 - b. *Cryptographic Length* [KMIP-SPEC] value :
 - i. 128-bit (combined with AES)
 - ii. 256-bit (combined with SHA, ECDH or ECDSA)
- 4. MAY support the following *Attributes* [KMIP-SPEC]
 - a. *Cryptographic Length* [KMIP-SPEC] value :
 - i. 256-bit (combined with AES)
 - ii. 384-bit bit (combined with SHA, ECDH or ECDSA)
- 5. SHALL support the following *Client-to-Server Operations* [KMIP-SPEC]:
 - a. *Create* [KMIP-SPEC]
 - b. *Create Key Pair* [KMIP-SPEC]
 - c. *Register* [KMIP-SPEC]
 - d. *Re-key* [KMIP-SPEC]
 - e. *Re-key Key Pair* [KMIP-SPEC]
- 6. SHALL support the following *Message Encoding* [KMIP-SPEC]:
 - a. *Recommended Curve Enumeration* [KMIP-SPEC] value:
 - i. P-256 (SECP256R1)
 - b. *Certificate Type Enumeration* [KMIP-SPEC] value:
 - i. X.509
 - c. *Cryptographic Algorithm Enumeration* [KMIP-SPEC] value:
 - i. AES
 - ii. ECDSA
 - iii. ECDH
 - iv. HMAC-SHA256
 - d. *Hashing Algorithm Enumeration* [KMIP-SPEC]
 - i. SHA-256
 - e. *Object Type Enumeration* [KMIP-SPEC] value:
 - i. Certificate
 - ii. Symmetric Key
 - iii. Public Key
 - iv. Private Key
 - f. *Key Format Type Enumeration* [KMIP-SPEC] value:
 - i. Raw
 - ii. ECPrivateKey
 - iii. X.509
 - iv. Transparent ECDSA Private Key
 - v. Transparent ECDSA Public Key
 - vi. Transparent ECDH Private Key

- vii. Transparent ECDH Public Key
 - g. *Digital Signature Algorithm Enumeration* [KMIP-SPEC] value:
 - i. ECDSA with SHA256 (on P-256)
- 7. MAY support the following *Message Encoding* [KMIP-SPEC]:
 - a. *Recommended Curve* [KMIP-SPEC] value:
 - i. P-384 (SECP384R1)
 - b. *Cryptographic Algorithm Enumeration* [KMIP-SPEC] value:
 - i. HMAC-SHA384
 - c. *Hashing Algorithm Enumeration* [KMIP-SPEC]
 - i. SHA-384
 - d. Digital Signature Algorithm Enumeration
 - i. ECDSA with SHA384 (on P-384)
- 8. SHALL support the Suite B minLOS_128 Test Cases returning results in accordance with the test cases.
- 9. MAY support any clause within [KMIP-SPEC] provided it does not conflict with any other clause within this section 2.2.
- 10. MAY support extensions outside the scope of this standard (e.g., vendor extensions, conformance clauses) that do not conflict with any KMIP or [CNSSP-15] requirements.

189 **3 Suite B minLOS_128 Test Cases**

190 **3.1 Mandatory Test Cases**

191 This section documents the test cases that a client or server conformant to this profile SHALL support.

192 N/A

4 Suite B minLOS_192 Profile

The Suite B minLOS_192 Profile describes a KMIP client interacting with a KMIP server as an information assurance product to provide a minimum level of security of 192 bits.
(http://www.nsa.gov/ia/programs/suiteb_cryptography/)

4.1 Authentication Suite

Implementations conformant to this profile SHALL use TLS to negotiate a mutually-authenticated connection.

4.1.1 Protocols

Conformant KMIP clients and servers SHALL support:

- TLS v1.2 [RFC5246]

4.1.2 Cipher Suites

Conformant KMIP servers SHALL support the following cipher suites:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

4.1.3 Client Authenticity

Conformant KMIP servers and clients SHALL handle client authenticity in accordance with section 3.2.3 of the TLS 1.2 Authentication Suite [KMIP-PROF].

4.1.4 Object Owner

Conformant KMIP servers and clients SHALL handle object owner in accordance with section 3.2.4 of the TLS 1.2 Authentication Suite [KMIP-PROF].

4.1.5 KMIP Port Number

Conformant KMIP servers and clients SHALL handle the KMIP port number in accordance with section 3.2.5 of the TLS 1.2 Authentication Suite [KMIP-PROF].

4.2 Suite B minLOS_192

KMIP clients conformant to this profile under [KMIP-SPEC]:

1. SHALL conform to the Baseline Client conformance clauses in [KMIP-PROF] and [KMIP-SPEC]
2. SHALL restrict use of the enumerated types listed in item 5 of the server list below to the values noted against each item
3. MAY support any clause within [KMIP-SPEC] provided it does not conflict with any other clause within this section 4.2.
4. MAY support extensions outside the scope of this standard (e.g., vendor extensions, conformance clauses) that do not conflict with any KMIP or [CNSSP-15] requirements.

KMIP servers conformant to this profile under [KMIP-SPEC]:

1. SHALL conform to the Baseline Server profile in [KMIP-PROF] and [KMIP-SPEC] and
2. SHALL support the following *Objects* [KMIP-SPEC]
 - a. *Certificate* [KMIP-SPEC]

- 229 b. *Symmetric Key* [KMIP-SPEC]
- 230 c. *Public Key* [KMIP-SPEC]
- 231 d. *Private Key* [KMIP-SPEC]
- 232 3. SHALL support the following *Attributes* [KMIP-SPEC]
- 233 a. *Cryptographic Algorithm* [KMIP-SPEC]
- 234 b. *Cryptographic Length* [KMIP-SPEC] value:
- 235 i. 384-bit bit (combined with SHA, ECDH or ECDSA)
- 236 4. SHALL support the following *Client-to-Server Operations* [KMIP-SPEC]:
- 237 a. *Create* [KMIP-SPEC]
- 238 b. *Create Key Pair* [KMIP-SPEC]
- 239 c. *Register* [KMIP-SPEC]
- 240 d. *Re-key* [KMIP-SPEC]
- 241 e. *Re-key Key Pair* [KMIP-SPEC]
- 242 5. SHALL support the following *Message Encoding* [KMIP-SPEC]:
- 243 a. *Recommended Curve Enumeration* [KMIP-SPEC] value:
- 244 i. P-384 (SECP384R1)
- 245 b. *Certificate Type Enumeration* [KMIP-SPEC] value:
- 246 i. X.509
- 247 c. *Cryptographic Algorithm Enumeration* [KMIP-SPEC] value:
- 248 i. AES
- 249 ii. ECDSA
- 250 iii. ECDH
- 251 iv. HMAC-SHA384
- 252 d. *Hashing Algorithm Enumeration* [KMIP-SPEC]
- 253 i. SHA-384
- 254 e. *Object Type Enumeration* [KMIP-SPEC] value:
- 255 i. Certificate
- 256 ii. Symmetric Key
- 257 iii. Public Key
- 258 iv. Private Key
- 259 f. *Key Format Type Enumeration* [KMIP-SPEC] value:
- 260 i. Raw
- 261 ii. ECPrivateKey
- 262 iii. X.509
- 263 iv. Transparent ECDSA Private Key
- 264 v. Transparent ECDSA Public Key
- 265 vi. Transparent ECDH Private Key
- 266 vii. Transparent ECDH Public Key
- 267 g. *Digital Signature Algorithm Enumeration* [KMIP-SPEC] value:
- 268 i. ECDSA with SHA384 (on P-384)
- 269 6. SHALL support the Suite B minLOS_192 Test Cases returning results in accordance with the test
- 270 cases.

- 271 7. MAY support any clause within [KMIP-SPEC] provided it does not conflict with any other clause
272 within this section 4.2.
- 273 8. MAY support extensions outside the scope of this standard (e.g., vendor extensions,
274 conformance clauses) that do not conflict with any KMIP or [CNSSP-15] requirements.

275 **5 Suite B minLOS_192 Test Cases**

276 **5.1 Mandatory Test Cases**

277 This section documents the test cases that a client or server conformant to this profile SHALL support.

278

279 N/A

6 Conformance

6.1 Suite B minLOS_128 Profile Conformance

KMIP client and server implementations conformant to this profile:

1. SHALL support the Authentication Suite conditions as specified in Section 2.1 of this profile.
2. SHALL support the conditions as specified in Section 2.2 of this profile.

6.2 Suite B minLOS_192 Profile Conformance

KMIP client and server implementations conformant to this profile:

1. SHALL support the Authentication Suite conditions as specified in Section 4.1 of this profile.
2. SHALL support the conditions as specified in Section 4.2 of this profile.

6.3 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.

6.3.1 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

- 318 c. CompromiseDate
- 319 d. CompromiseOccurrenceDate
- 320 e. DeactivationDate
- 321 f. DestroyDate
- 322 g. InitialDate
- 323 h. LastChangeDate
- 324 i. ProtectStartDate
- 325 j. ProcessStopDate
- 326 k. ValidityDate
- 327 l. OriginalCreationDate
- 328 10. LinkedObjectIdentifier
- 329 11. DigestValue
 - 330 a. For those managed cryptographic objects which are dynamically generated
- 331 12. KeyFormatType
 - 332 a. The key format type selected by the server when it creates managed objects
- 333 13. Digest
 - 334 a. The HashingAlgorithm selected by the server when it calculates the digest for a managed
 - 335 object for which it has access to the key material
 - 336 b. The Digest Value
- 337 14. Extensions reported in Query for ExtensionList and ExtensionMap
- 338 15. Application Namespaces reported in Query
- 339 16. Object Types reported in Query other than those noted as required in this profile
- 340 17. Operation Types reported in Query other than those noted as required in this profile (or any
- 341 referenced profile documents)
- 342 18. For TextString attribute values containing test identifiers:
 - 343 a. Additional vendor or application prefixes
- 344 19. Additional attributes beyond those noted in the response

345

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

- 347 1. Object Group values – May or may not return one or more Object Group values not included in
- 348 the requests
- 349 2. y-CustomAttributes – May or may not include additional server-specific associated attributes not
- 350 included in requests
- 351 3. Message Extensions – May or may not include additional (non-critical) vendor extensions
- 352 4. TemplateAttribute – May or may not be included in responses where the Template Attribute
- 353 response is noted as optional in [KMIP-SPEC]
- 354 5. AttributeIndex – May or may not include Attribute Index value where the Attribute Index value is 0
- 355 for Protocol Versions 1.1 and above.
- 356 6. ResultMessage – May or may not be included in responses and the value (if included) may vary
- 357 from the text contained within the test case.
- 358 7. The list of Protocol Versions returned in a DiscoverVersion response may include additional
- 359 protocol versions if the request has not specified a list of client supported Protocol Versions.
- 360 8. VendorIdentification - The value (if included) may vary from the text contained within the test
- 361 case.

6.3.2 Variable behavior

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

1. A test may omit the clean-up requests and responses (containing Revoke and/or Destroy) at the end of the test provided there is a separate mechanism to remove the created objects during testing.
2. A test may omit the test identifiers if the client is unable to include them in requests. This includes the following attributes:
 - a. Name; and
 - b. x-ID

Appendix A. Acknowledgments

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

Participants:

373 Hal Aldridge, Sypris Electronics
374 Mike Allen, Symantec
375 Gordon Arnold, IBM
376 Todd Arnold, IBM
377 Richard Austin, Hewlett-Packard
378 Lars Bagnert, PrimeKey
379 Elaine Barker, NIST
380 Peter Bartok, Venafi, Inc.
381 Tom Benjamin, IBM
382 Anthony Berglas, Cryptsoft
383 Mathias Björkqvist, IBM
384 Kevin Bocket, Venafi
385 Anne Bolgert, IBM
386 Alan Brown, Thales e-Security
387 Tim Bruce, CA Technologies
388 Chris Burchett, Credant Technologies, Inc.
389 Kelley Burgin, National Security Agency
390 Robert Burns, Thales e-Security
391 Chuck Castleton, Venafi
392 Kenli Chong, QuintessenceLabs
393 John Clark, Hewlett-Packard
394 Tom Clifford, Symantec Corp.
395 Doron Cohen, SafeNet, Inc
396 Tony Cox, Cryptsoft
397 Russell Dietz, SafeNet, Inc
398 Graydon Dodson, Lexmark International Inc.
399 Vinod Duggirala, EMC Corporation
400 Chris Dunn, SafeNet, Inc.
401 Michael Duren, Sypris Electronics
402 James Dzierzanowski, American Express CCoE
403 Faisal Faruqui, Thales e-Security
404 Stan Feather, Hewlett-Packard
405 David Finkelstein, Symantec Corp.
406 James Fitzgerald, SafeNet, Inc.
407 Indra Fitzgerald, Hewlett-Packard
408 Judith Furlong, EMC Corporation
409 Susan Gleeson, Oracle
410 Robert Griffin, EMC Corporation
411 Paul Grojean, Individual
412 Robert Haas, IBM
413 Thomas Hardjono, M.I.T.
414 ChengDong He, Huawei Technologies Co., Ltd.
415 Steve He, Vormetric
416 Kurt Heberlein, Hewlett-Packard
417 Larry Hofer, Emulex Corporation
418 Maryann Hondo, IBM
419 Walt Hubis, NetApp
420 Tim Hudson, Cryptsoft
421 Jonas Iggbom, Venafi, Inc.

422 Sitaram Inguva, American Express CCoE
423 Jay Jacobs, Target Corporation
424 Glen Jaquette, IBM
425 Mahadev Karadiguddi, NetApp
426 Greg Kazmierczak, Wave Systems Corp.
427 Marc Kenig, SafeNet, Inc.
428 Mark Knight, Thales e-Security
429 Kathy Kriese, Symantec Corporation
430 Mark Lambiase, SecureAuth
431 John Leiseboer, Quintessence Labs
432 Hal Lockhart, Oracle Corporation
433 Robert Lockhart, Thales e-Security
434 Anne Luk, Cryptsoft
435 Sairam Manidi, Freescale
436 Luther Martin, Voltage Security
437 Neil McEvoy, iFOSSF
438 Marina Milshtein, Individual
439 Dale Moberg, Axway Software
440 Jishnu Mukeri, Hewlett-Packard
441 Bryan Olson, Hewlett-Packard
442 John Peck, IBM
443 Rob Philpott, EMC Corporation
444 Denis Pochuev, SafeNet, Inc.
445 Reid Poole, Venafi, Inc.
446 Ajai Puri, SafeNet, Inc.
447 Saravanan Ramalingam, Thales e-Security
448 Peter Reed, SafeNet, Inc.
449 Bruce Rich, IBM
450 Christina Richards, American Express CCoE
451 Warren Robbins, Dell
452 Peter Robinson, EMC Corporation
453 Scott Rotondo, Oracle
454 Saikat Saha, SafeNet, Inc.
455 Anil Saldhana, Red Hat
456 Subhash Sankuratipati, NetApp
457 Boris Schumperli, Cryptomathic
458 Greg Singh, QuintessenceLabs
459 David Smith, Venafi, Inc.
460 Brian Spector, Certivox
461 Terence Spies, Voltage Security
462 Deborah Steckroth, RouteOne LLC
463 Michael Stevens, QuintessenceLabs
464 Marcus Streets, Thales e-Security
465 Satish Sundar, IBM
466 Kiran Thota, VMware
467 Somanchi Trinath, Freescale Semiconductor, Inc.
468 Nathan Turajski, Thales e-Security
469 Sean Turner, IECA, Inc.
470 Paul Turner, Venafi, Inc.
471 Rod Wideman, Quantum Corporation
472 Steven Wierenga, Hewlett-Packard
473 Jin Wong, QuintessenceLabs
474 Sameer Yami, Thales e-Security
475 Peter Yee, EMC Corporation
476 Krishna Yellepeddy, IBM
477 Catherine Ying, SafeNet, Inc.
478 Tatu Ylonen, SSH Communications Security (Tectia Corp)

479 Michael Yoder, Vormetric. Inc.
480 Magda Zdunkiewicz, Cryptsoft
481 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.

482

Appendix C. Revision History

Revision	Date	Editor	Changes Made
wd01	10 July 2013	Kelley Burgin / Tim Hudson	Initial Draft
wd02	8 August 2013	Kelley Burgin	Editorial updates and inclusion of a corresponding restriction on client enumeration usage
wd03	10 August 2013	Tim Hudson	Updated Permitted Test Case Variations
wd03a	24-October- 2013	Tim Hudson	Editorial update to include VendorIdentification in the list of allowed variations as per TC motion.