

Key Management Interoperability Protocol Profiles Version 1.2

Committee Specification Draft 02

19 June 2014

Specification URIs

This version:

<http://docs.oasis-open.org/kmip/profiles/v1.2/csd02/kmip-profiles-v1.2-csd02.doc> (Authoritative)
<http://docs.oasis-open.org/kmip/profiles/v1.2/csd02/kmip-profiles-v1.2-csd02.html>
<http://docs.oasis-open.org/kmip/profiles/v1.2/csd02/kmip-profiles-v1.2-csd02.pdf>

Previous version:

<http://docs.oasis-open.org/kmip/profiles/v1.2/csprd01/kmip-profiles-v1.2-csprd01.doc>
(Authoritative)
<http://docs.oasis-open.org/kmip/profiles/v1.2/csprd01/kmip-profiles-v1.2-csprd01.html>
<http://docs.oasis-open.org/kmip/profiles/v1.2/csprd01/kmip-profiles-v1.2-csprd01.pdf>

Latest version:

<http://docs.oasis-open.org/kmip/profiles/v1.2/kmip-profiles-v1.2.doc> (Authoritative)
<http://docs.oasis-open.org/kmip/profiles/v1.2/kmip-profiles-v1.2.html>
<http://docs.oasis-open.org/kmip/profiles/v1.2/kmip-profiles-v1.2.pdf>

Technical Committee:

OASIS Key Management Interoperability Protocol (KMIP) TC

Chairs:

Subhash Sankuratripati (Subhash.Sankuratripati@netapp.com), NetApp
Saikat Saha (saikat.saha@oracle.com), Oracle

Editors:

Tim Hudson (tjh@cryptsoft.com), Cryptsoft Pty Ltd.
Robert Lockhart (Robert.Lockhart@thalessec.com), Thales e-Security

Related work:

This specification replaces or supersedes:

- *Key Management Interoperability Protocol Profiles Version 1.1*. Edited by Robert Griffin and Subhash Sankuratripati. Latest version <http://docs.oasis-open.org/kmip/profiles/v1.1/kmip-profiles-v1.1.html>.

This specification is related to:

- *Key Management Interoperability Protocol Specification Version 1.2*. Edited by Kiran Thota and Kelley Burgin. Latest version. <http://docs.oasis-open.org/kmip/spec/v1.2/kmip-spec-v1.2.html>.
- *Key Management Interoperability Protocol Test Cases Version 1.2*. Edited by Tim Hudson and Faisal Faruqui. Latest version. <http://docs.oasis-open.org/kmip/testcases/v1.2/kmip-testcases-v1.2.html>.
- *Key Management Interoperability Protocol Use Cases Version 1.2*. Work in progress. To be published at: <http://docs.oasis-open.org/kmip/usecases/>.
- *Key Management Interoperability Protocol Usage Guide Version 1.2*. Edited by Indra Fitzgerald and Judith Furlong. Latest version. <http://docs.oasis-open.org/kmip/ug/v1.2/kmip-ug-v1.2.html>.

Abstract:

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

Status:

This document was last revised or approved by the OASIS Key Management Interoperability Protocol (KMIP) TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document.

Technical Committee members should send comments on this 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 <https://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 (<https://www.oasis-open.org/committees/kmip/ipr.php>).

Citation format:

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

[KMIP-Profiles]

Key Management Interoperability Protocol Profiles Version 1.2. Edited by Tim Hudson and Robert Lockhart. 19 June 2014. OASIS Committee Specification Draft 02. <http://docs.oasis-open.org/kmip/profiles/v1.2/csd02/kmip-profiles-v1.2-csd02.html>. Latest version: <http://docs.oasis-open.org/kmip/profiles/v1.2/kmip-profiles-v1.2.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 <https://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.....	5
2	Profiles.....	6
2.1	Guidelines for Specifying Conformance Clauses.....	6
2.2	Guidelines for Specifying Authentication Suites.....	6
2.3	Guidelines for Specifying KMIP Profiles.....	6
2.4	Guidelines for Validating Conformance to KMIP Server Profiles.....	6
2.5	Guidelines for Validating Conformance to KMIP Client Profiles.....	6
3	Authentication Suites.....	8
3.1	Basic Authentication Suite.....	8
3.1.1	Protocols.....	8
3.1.2	Cipher Suites.....	8
3.1.3	Client Authenticity.....	9
3.1.4	KMIP Port Number.....	9
3.2	TLS 1.2 Authentication Suite.....	9
3.2.1	Protocols.....	10
3.2.2	Cipher Suites.....	10
3.2.3	Client Authenticity.....	10
3.2.4	KMIP Port Number.....	10
4	KMIP Profiles.....	11
4.1	Baseline Server Basic KMIP Profile.....	11
4.2	Baseline Server TLS v1.2 KMIP Profile.....	11
4.3	Baseline Client Basic KMIP Profile.....	11
4.4	Baseline Client TLS v1.2 KMIP Profile.....	11
4.5	Complete Server Basic KMIP Profile.....	11
4.6	Complete Server TLS v1.2 KMIP Profile.....	11
5	Conformance.....	12
5.1	Baseline Server.....	12
5.2	Baseline Client.....	13
5.3	Complete Server.....	14
Appendix A.	Acknowledgments.....	15
Appendix B.	Revision History.....	18

1 Introduction

OASIS requires a conformance section in an approved committee specification ([KMIP-SPEC] [TC-PROC], section 2.18 Work Product Quality, paragraph 8a):

A specification that is approved by the TC at the Public Review Draft, Committee Specification or OASIS Standard level must include a separate section, listing a set of numbered conformance clauses, to which any implementation of the specification must adhere in order to claim conformance to the specification (or any optional portion thereof).

This document intends to meet this OASIS requirement on conformance clauses for a KMIP server or KMIP client ([KMIP-SPEC] 12.1, 12.2) through profiles that define the use of KMIP objects, attributes, operations, message elements and authentication methods within specific contexts of KMIP server and client interaction.

These profiles define a set of normative constraints for employing KMIP within a particular environment or context of use. They may, optionally, require the use of specific KMIP functionality or in other respects define the processing rules to be followed by profile actors.

For normative definition of the elements of KMIP specified in these profiles, see the [KMIP Specification](#) ([KMIP-SPEC]).

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].

1.2 Normative References

- | | |
|-------------|--|
| [KMIP-SPEC] | <i>Key Management Interoperability Protocol Specification Version 1.2. XX MMM 2013. Candidate OASIS Standard 01. URL.</i> |
| [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 & C.Allen, <i>The TLS Protocol, Version 1.0</i> , http://www.ietf.org/rfc/rfc2246.txt , IETF RFC 2246, January 1999 |
| [RFC3268] | P. Chown, <i>Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)</i> , http://www.ietf.org/rfc/rfc3268.txt , IETF RFC 3268, June 2002 |
| [RFC4346] | T. Dierks & E. Rescorla, <i>The Transport Layer Security (TLS) Protocol, Version 1.1</i> , http://www.ietf.org/rfc/rfc4346.txt , IETF RFC 4346, April 2006 |
| [RFC5246] | T. Dierks & E. Rescorla, <i>The Transport Layer Security (TLS) Protocol, Version 1.2</i> , http://www.ietf.org/rfc/rfc5246.txt , IETF RFC 5246, August 2008 |

1.3 Non-Normative References

- | | |
|-----------|--|
| [TC-PROC] | <i>OASIS TC Process</i> . 14 February 2013. OASIS Process. https://www.oasis-open.org/policies-guidelines/tc-process . |
|-----------|--|

38 2 Profiles

39 This document defines a selected set of conformance clauses and authentication suites which when
40 combined form KMIP Profiles.

41 2.1 Guidelines for Specifying Conformance Clauses

42 This section provides a checklist of issues that SHALL be addressed by each clause.

- 43 1. Implement functionality as mandated by [KMIP-SPEC] Section 12 (Conformance clauses for a
44 KMIP server or a KMIP client)
- 45 2. Specify the list of additional objects that SHALL be supported
- 46 3. Specify the list of additional attributes that SHALL be supported
- 47 4. Specify the list of additional operations that SHALL be supported
- 48 5. Specify any additional message content that SHALL be supported

49 2.2 Guidelines for Specifying Authentication Suites

- 50 1. Channel Security – For all operations, communication between client and server SHALL
51 establish and maintain channel confidentiality and integrity,.
- 52 2. Channel Options – Options like protocol version and cipher suite
- 53 3. Server and Client Authenticity – For all operations, communication between client and server
54 SHALL provide assurance of server authenticity and client authenticity

55 2.3 Guidelines for Specifying KMIP Profiles

56 Any vendor or organization, such as other standards bodies, MAY create a KMIP Profile and publish it.

- 57 1. The profile SHALL be publicly available.
- 58 2. The KMIP Technical Committee SHALL be formally advised of the availability of the profile and
59 the location of the published profile.
- 60 3. The profile SHALL be defined as a tuple of {Conformance Clause, Authentication Suite}.
- 61 4. The KMIP Technical Committee SHOULD review the profile prior to publication.

62 2.4 Guidelines for Validating Conformance to KMIP Server Profiles

63 A KMIP server implementation SHALL claim conformance to a specific server profile only if it supports all
64 required objects, operations, messaging and attributes of that profile

- 65 1. All objects specified as required in that profile
- 66 2. All operations specified as required in that profile
- 67 3. All attributes specified as required in that profile
- 68 4. The defined wire protocols (TLS, SSL, IPSec, etc...) for that profile
- 69 5. The defined methods of authentication for that profile

70 2.5 Guidelines for Validating Conformance to KMIP Client Profiles

71 A KMIP client implementation SHALL claim conformance to a specific client profile only if it supports all
72 required objects, operations, messaging and attributes of that profile

- 73 1. All objects specified as required in that profile
- 74 2. All operations specified as required in that profile
- 75 3. All attributes specified as required in that profile
- 76 4. The defined wire protocols (TLS, SSL, IPSec, etc...) for that profile
- 77 5. The defined methods of authentication for that profile
- 78

79 3 Authentication Suites

80 This section contains the list of protocol versions and cipher suites that are to be used by profiles
81 contained within this document.

82 3.1 Basic Authentication Suite

83 This authentication set stipulates that a conformant KMIP client or server SHALL use TLS to negotiate a
84 secure connection.

85 3.1.1 Protocols

86 Conformant KMIP clients or servers SHALL support:

- 87 • TLS v1.0 [RFC2246] and [RFC3268]

88 Conformant KMIP clients or servers MAY support:

- 89 • TLS v1.1 [RFC4346]
- 90 • TLS v1.2 [RFC5246]

91 Conformant KMIP clients or servers SHALL NOT support:

- 92 • SSL v3.0
- 93 • SSL v2.0
- 94 • SSL v1.0

95 3.1.2 Cipher Suites

96 Conformant KMIP clients or servers SHALL support the following cipher suites:

- 97 • TLS_RSA_WITH_AES_128_CBC_SHA

98 Conformant KMIP clients and servers MAY support the following cipher suites:

- 99 • TLS_RSA_WITH_3DES_EDE_CBC_SHA
- 100 • TLS_RSA_WITH_AES_128_CBC_SHA256
- 101 • TLS_RSA_WITH_AES_256_CBC_SHA
- 102 • TLS_RSA_WITH_AES_256_CBC_SHA256
- 103 • TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
- 104 • TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
- 105 • TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- 106 • TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- 107 • TLS_DH_DSS_WITH_AES_128_CBC_SHA
- 108 • TLS_DH_RSA_WITH_AES_128_CBC_SHA
- 109 • TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- 110 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- 111 • TLS_DH_DSS_WITH_AES_256_CBC_SHA
- 112 • TLS_DH_RSA_WITH_AES_256_CBC_SHA
- 113 • TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- 114 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- 115 • TLS_DH_DSS_WITH_AES_128_CBC_SHA256
- 116 • TLS_DH_RSA_WITH_AES_128_CBC_SHA256
- 117 • TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- 118 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- 119 • TLS_DH_DSS_WITH_AES_256_CBC_SHA256
- 120 • TLS_DH_RSA_WITH_AES_256_CBC_SHA256
- 121 • TLS_DHE_DSS_WITH_AES_256_CBC_SHA256

- 122 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- 123 • TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
- 124 • TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- 125 • TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- 126 • TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- 127 • TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- 128 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- 129 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- 130 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- 131 • TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
- 132 • TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- 133 • TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- 134 • TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- 135 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- 136 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- 137 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- 138 • TLS_PSK_WITH_3DES_EDE_CBC_SHA
- 139 • TLS_PSK_WITH_AES_128_CBC_SHA
- 140 • TLS_PSK_WITH_AES_256_CBC_SHA
- 141 • TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA
- 142 • TLS_DHE_PSK_WITH_AES_128_CBC_SHA
- 143 • TLS_DHE_PSK_WITH_AES_256_CBC_SHA
- 144 • TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA
- 145 • TLS_RSA_PSK_WITH_AES_128_CBC_SHA
- 146 • TLS_RSA_PSK_WITH_AES_256_CBC_SHA
- 147 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- 148 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- 149 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- 150 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

151 Conformant KMIP clients or servers SHALL NOT support any cipher suite not listed above.

152 NOTE: TLS 1.0 has known security issues and implementations that need protections against known
153 issues SHOULD considering using the TLS 1.2 Authentication Suite (3.2)

154 3.1.3 Client Authenticity

155 Conformant KMIP servers SHALL require the use of channel (TLS) mutual authentication to provide
156 assurance of client authenticity for all operations other than:

- 157 • Query
- 158 • Discover Versions

159 Conformant KMIP servers SHALL use the identity derived from the channel mutual authentication to
160 determine the client identity if the KMIP client requests do not contain an Authentication object.

161 Conformant KMIP servers SHALL use the identity derived from the channel mutual authentication along
162 with the Credential information to determine the client identity if the KMIP client requests contain an
163 Authentication object.

164 The exact mechanisms determining the client identity are outside the scope of this specification.

165 3.1.4 KMIP Port Number

166 Conformant KMIP servers SHOULD use TCP port number 5696, as assigned by IANA.

167 3.2 TLS 1.2 Authentication Suite

168 This authentication set stipulates that a conformant KMIP client and server SHALL use TLS to negotiate a
169 mutually-authenticated connection.

170 **3.2.1 Protocols**

171 Conformant KMIP clients and servers SHALL support:

- 172
 - TLS v1.2 [RFC2246]

173 **3.2.2 Cipher Suites**

174 Conformant KMIP servers SHALL support the following cipher suites:

- 175
 - TLS_RSA_WITH_AES_256_CBC_SHA256
 - TLS_RSA_WITH_AES_128_CBC_SHA256

177

178 Conformant KMIP servers and clients MAY support the cipher suites specified as MAY in section 3.2.2 of
179 the Basic Authentication Suite.

180 **3.2.3 Client Authenticity**

181 Conformant KMIP servers and clients SHALL handle client authenticity in accordance with section 3.2.3
182 of the Basic Authentication Suite.

183 **3.2.4 KMIP Port Number**

184 Conformant KMIP servers and clients SHALL handle the KMIP port number in accordance with section
185 3.1.4 of the Basic Authentication Suite.

186 **4 KMIP Profiles**

187 This section lists the KMIP profiles that are defined in this specification.

188 A KMIP server or KMIP client MAY support more than one profile at the same time provided there are no
189 conflicting requirements between any of the supported profiles.

190 **4.1 Baseline Server Basic KMIP Profile**

191 The profile that consists of the tuple {Baseline Server, Basic Authentication Suite}.

192 **4.2 Baseline Server TLS v1.2 KMIP Profile**

193 A profile that consists of the tuple {Baseline Server, TLS 1.2 Authentication Suite}.

194 **4.3 Baseline Client Basic KMIP Profile**

195 The profile that consists of the tuple {Baseline Client, Basic Authentication Suite}.

196 **4.4 Baseline Client TLS v1.2 KMIP Profile**

197 A profile that consists of the tuple {Baseline Client, TLS 1.2 Authentication Suite}.

198 **4.5 Complete Server Basic KMIP Profile**

199 The profile that consists of the tuple {Complete Server, Basic Authentication Suite}.

200 **4.6 Complete Server TLS v1.2 KMIP Profile**

201 A profile that consists of the tuple {Complete Server, TLS 1.2 Authentication Suite}.

202

203 5 Conformance

204 The baseline server and client profiles provide the most basic functionality that is expected of a
205 conformant KMIP client or server. The complete server profile defines a KMIP server that implements the
206 entire specification. A KMIP implementation conformant to this specification (the Key Management
207 Interoperability Protocol Profiles) SHALL meet all the conditions documented in one or more of the
208 following sections.

209 Specific combinations of KMIP objects, operations, messaging and attributes beyond those defined in the
210 following sections are specified in separate profile documents.

211 5.1 Baseline Server

212 The Baseline Server provides the most basic functionality that is expected of a conformant KMIP server –
213 the ability to provide information about the server and the managed objects supported by the server.

214 An implementation is a conforming Baseline Server if it meets the following conditions:

- 215 1. Supports the conditions required by the KMIP Server conformance clauses ([KMIP-SPEC] 12.1)
- 216 2. Supports the following objects:
 - 217 a. Attribute ([KMIP-SPEC] 2.1.1)
 - 218 b. Credential ([KMIP-SPEC] 2.1.2)
 - 219 c. Key Block ([KMIP-SPEC] 2.1.3)
 - 220 d. Key Value ([KMIP-SPEC] 2.1.4)
 - 221 e. Template-Attribute Structure ([KMIP-SPEC] 2.1.8)
 - 222 f. Extension Information ([KMIP-SPEC] 2.1.9)
- 223 3. Supports the following subsets of attributes:
 - 224 a. Unique Identifier ([KMIP-SPEC] 3.1)
 - 225 b. Name ([KMIP-SPEC] 3.2)
 - 226 c. Object Type ([KMIP-SPEC] 3.3)
 - 227 d. Cryptographic Algorithm ([KMIP-SPEC] 3.4)
 - 228 e. Cryptographic Length ([KMIP-SPEC] 3.5)
 - 229 f. Cryptographic Parameters ([KMIP-SPEC] 3.6)
 - 230 g. Digest ([KMIP-SPEC] 3.17)
 - 231 h. Default Operation Policy ([KMIP-SPEC] 3.18.2)
 - 232 i. Cryptographic Usage Mask ([KMIP-SPEC] 3.19)
 - 233 j. State ([KMIP-SPEC] 3.22)
 - 234 k. Initial Date ([KMIP-SPEC] 3.23)
 - 235 l. Activation Date ([KMIP-SPEC] 3.24)
 - 236 m. Deactivation Date ([KMIP-SPEC] 3.27)
 - 237 n. Compromise Occurrence Date ([KMIP-SPEC] 3.29)
 - 238 o. Compromise Date ([KMIP-SPEC] 3.30)
 - 239 p. Revocation Reason ([KMIP-SPEC] 3.31)
 - 240 q. Last Change Date ([KMIP-SPEC] 3.38)
- 241 4. Supports the ID Placeholder ([KMIP-SPEC] 4)
- 242 5. Supports the following client-to-server operations:
 - 243 a. Locate ([KMIP-SPEC] 4.9)
 - 244 b. Check ([KMIP-SPEC] 4.10)
 - 245 c. Get ([KMIP-SPEC] 4.11)
 - 246 d. Get Attributes ([KMIP-SPEC] 4.12)
 - 247 e. Get Attribute List ([KMIP-SPEC] 4.13)
 - 248 f. Add Attribute ([KMIP-SPEC] 4.14)
 - 249 g. Modify Attribute ([KMIP-SPEC] 4.15)
 - 250 h. Delete Attribute ([KMIP-SPEC] 4.16)

- 251 i. Activate ([KMIP-SPEC] 4.19)
- 252 j. Revoke ([KMIP-SPEC] 4.20)
- 253 k. Destroy ([KMIP-SPEC] 4.21)
- 254 l. Query ([KMIP-SPEC] 4.25)
- 255 m. Discover Versions ([KMIP-SPEC] 4.26)
- 256 6. Supports the following message contents:
 - 257 a. Protocol Version ([KMIP-SPEC] 6.1)
 - 258 b. Operation ([KMIP-SPEC] 6.2)
 - 259 c. Maximum Response Size ([KMIP-SPEC] 6.3)
 - 260 d. Unique Batch Item ID ([KMIP-SPEC] 6.4)
 - 261 e. Time Stamp ([KMIP-SPEC] 6.5)
 - 262 f. Asynchronous Indicator ([KMIP-SPEC] 6.7)
 - 263 g. Result Status ([KMIP-SPEC] 6.9)
 - 264 h. Result Reason ([KMIP-SPEC] 6.10)
 - 265 i. Batch Order Option ([KMIP-SPEC] 6.12)
 - 266 j. Batch Error Continuation Option ([KMIP-SPEC] 6.13)
 - 267 k. Batch Count ([KMIP-SPEC] 6.14)
 - 268 l. Batch Item ([KMIP-SPEC] 6.15)
 - 269 m. Attestation Capable Indicator ([KMIP-SPEC] 6.17)
- 270 7. Supports Message Format ([KMIP-SPEC] 7)
- 271 8. Supports Authentication ([KMIP-SPEC] 8)
- 272 9. Supports the TTLV encoding ([KMIP-SPEC] 9.1)
- 273 10. Supports the transport requirements ([KMIP-SPEC] 10)
- 274 11. Supports Error Handling ([KMIP-SPEC] 11) for any supported object, attribute, or operation
- 275 12. Optionally supports any clause within [KMIP-SPEC] that is not listed above
- 276 13. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions,
- 277 conformance clauses) that do not contradict any KMIP requirements

278 5.2 Baseline Client

279 The Baseline Client provides some of the most basic functionality that is expected of a conformant KMIP
 280 client – the ability to request information about the server.

281 An implementation is a conforming Baseline Client Clause if it meets the following conditions:

- 282 1. Supports the conditions required by the KMIP Client conformance clauses ([KMIP-SPEC] 12.2)
- 283 2. Supports the following objects:
 - 284 a. Attribute ([KMIP-SPEC] 2.1.1)
 - 285 b. Template-Attribute Structure ([KMIP-SPEC] 2.1.8)
- 286 3. Supports the following subsets of attributes:
 - 287 a. Unique Identifier ([KMIP-SPEC] 3.1)
 - 288 b. Object Type ([KMIP-SPEC] 3.3)
 - 289 c. Digest ([KMIP-SPEC] 3.17)
 - 290 d. Default Operation Policy ([KMIP-SPEC] 3.18.2)
 - 291 e. State ([KMIP-SPEC] 3.22)
 - 292 f. Initial Date ([KMIP-SPEC] 3.23)
 - 293 g. Activation Date ([KMIP-SPEC] 3.24)
 - 294 h. Deactivation Date ([KMIP-SPEC] 3.27)
 - 295 i. Last Change Date ([KMIP-SPEC] 3.38)
- 296 4. Supports the ID Placeholder ([KMIP-SPEC] 4)
- 297 5. Supports the following client-to-server operations:
 - 298 a. Locate ([KMIP-SPEC] 4.9)
 - 299 b. Get ([KMIP-SPEC] 4.11)

- 300 c. Get Attributes ([KMIP-SPEC] 4.12)
- 301 d. Query ([KMIP-SPEC] 4.25)
- 302 6. Supports the following message contents:
 - 303 a. Protocol Version ([KMIP-SPEC] 6.1)
 - 304 b. Operation ([KMIP-SPEC] 6.2)
 - 305 c. Maximum Response Size ([KMIP-SPEC] 6.3)
 - 306 d. Unique Batch Item ID ([KMIP-SPEC] 6.4)
 - 307 e. Time Stamp ([KMIP-SPEC] 6.5)
 - 308 f. Asynchronous Indicator ([KMIP-SPEC] 6.7)
 - 309 g. Result Status ([KMIP-SPEC] 6.9)
 - 310 h. Result Reason ([KMIP-SPEC] 6.10)
 - 311 i. Batch Order Option ([KMIP-SPEC] 6.12)
 - 312 j. Batch Error Continuation Option ([KMIP-SPEC] 6.13)
 - 313 k. Batch Count ([KMIP-SPEC] 6.14)
 - 314 l. Batch Item ([KMIP-SPEC] 6.15)
- 315 14. Supports Message Format ([KMIP-SPEC] 7)
- 316 15. Supports Authentication ([KMIP-SPEC] 8)
- 317 16. Supports the TTLV encoding ([KMIP-SPEC] 9.1)
- 318 17. Supports the transport requirements ([KMIP-SPEC] 10)
- 319 18. Supports Error Handling ([KMIP-SPEC] 11) for any supported object, attribute, or operation
- 320 19. Optionally supports any clause within [KMIP-SPEC] that is not listed above.
- 321 20. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions,
- 322 conformance clauses) that do not contradict any KMIP requirements

323 5.3 Complete Server

324 The Complete Server provides functionality that is expected of a conformant KMIP server that implements
325 the entire specification.

326 An implementation is a conforming Complete Server if it meets the following conditions:

- 327 1. Supports KMIP Server conformance clauses ([KMIP-SPEC] 12.1)
- 328 2. Supports Objects ([KMIP-SPEC] 2)
- 329 3. Supports Attributes ([KMIP-SPEC] 3)
- 330 4. Supports Client-to-Server operations ([KMIP-SPEC] 4)
- 331 5. Supports Server-to-Client operations ([KMIP-SPEC] 5)
- 332 6. Supports Message Contents ([KMIP-SPEC] 6)
- 333 7. Supports Message Formats ([KMIP-SPEC] 7)
- 334 8. Supports Authentication ([KMIP-SPEC] 8)
- 335 9. Supports Message Encodings ([KMIP-SPEC] 9)
- 336 10. Supports Error Handling ([KMIP-SPEC] 11)
- 337 11. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions,
- 338 conformance clauses) that do not contradict any KMIP requirements

339

340 Appendix A. Acknowledgments

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

343 **Participants:**

344 Hal Aldridge, Sypris Electronics
345 Mike Allen, Symantec
346 Gordon Arnold, IBM
347 Todd Arnold, IBM
348 Richard Austin, Hewlett-Packard
349 Lars Bagnert, PrimeKey
350 Elaine Barker, NIST
351 Peter Bartok, Venafi, Inc.
352 Tom Benjamin, IBM
353 Anthony Berglas, Cryptsoft
354 Mathias Björkqvist, IBM
355 Kevin Bocket, Venafi
356 Anne Bolgert, IBM
357 Alan Brown, Thales e-Security
358 Tim Bruce, CA Technologies
359 Chris Burchett, Credant Technologies, Inc.
360 Kelley Burgin, National Security Agency
361 Robert Burns, Thales e-Security
362 Chuck Castleton, Venafi
363 Kenli Chong, QuintessenceLabs
364 John Clark, Hewlett-Packard
365 Tom Clifford, Symantec Corp.
366 Doron Cohen, SafeNet, Inc
367 Tony Cox, Cryptsoft
368 Russell Dietz, SafeNet, Inc
369 Graydon Dodson, Lexmark International Inc.
370 Vinod Duggirala, EMC Corporation
371 Chris Dunn, SafeNet, Inc.
372 Michael Duren, Sypris Electronics
373 James Dzierzanowski, American Express CCoE
374 Faisal Faruqui, Thales e-Security
375 Stan Feather, Hewlett-Packard
376 David Finkelstein, Symantec Corp.
377 James Fitzgerald, SafeNet, Inc.
378 Indra Fitzgerald, Hewlett-Packard
379 Judith Furlong, EMC Corporation
380 Susan Gleeson, Oracle
381 Robert Griffin, EMC Corporation
382 Paul Grojean, Individual
383 Robert Haas, IBM
384 Thomas Hardjono, M.I.T.
385 ChengDong He, Huawei Technologies Co., Ltd.
386 Steve He, Vormetric
387 Kurt Heberlein, Hewlett-Packard
388 Larry Hofer, Emulex Corporation
389 Maryann Hondo, IBM
390 Walt Hubis, NetApp
391 Tim Hudson, Cryptsoft
392 Jonas Iggbom, Venafi, Inc.

393 Sitaram Inguva, American Express CCoE
394 Jay Jacobs, Target Corporation
395 Glen Jaquette, IBM
396 Mahadev Karadiguddi, NetApp
397 Greg Kazmierczak, Wave Systems Corp.
398 Marc Kenig, SafeNet, Inc.
399 Mark Knight, Thales e-Security
400 Kathy Kriese, Symantec Corporation
401 Mark Lambiase, SecureAuth
402 John Leiseboer, Quintessence Labs
403 Hal Lockhart, Oracle Corporation
404 Robert Lockhart, Thales e-Security
405 Anne Luk, Cryptsoft
406 Sairam Manidi, Freescale
407 Luther Martin, Voltage Security
408 Neil McEvoy, iFOSSF
409 Marina Milshtein, Individual
410 Dale Moberg, Axway Software
411 Jishnu Mukeri, Hewlett-Packard
412 Bryan Olson, Hewlett-Packard
413 John Peck, IBM
414 Rob Philpott, EMC Corporation
415 Denis Pochuev, SafeNet, Inc.
416 Reid Poole, Venafi, Inc.
417 Ajai Puri, SafeNet, Inc.
418 Saravanan Ramalingam, Thales e-Security
419 Peter Reed, SafeNet, Inc.
420 Bruce Rich, IBM
421 Christina Richards, American Express CCoE
422 Warren Robbins, Dell
423 Peter Robinson, EMC Corporation
424 Scott Rotondo, Oracle
425 Saikat Saha, SafeNet, Inc.
426 Anil Saldhana, Red Hat
427 Subhash Sankuratripati, NetApp
428 Boris Schumperli, Cryptomathic
429 Greg Singh, QuintessenceLabs
430 David Smith, Venafi, Inc
431 Brian Spector, Certivox
432 Terence Spies, Voltage Security
433 Deborah Steckroth, RouteOne LLC
434 Michael Stevens, QuintessenceLabs
435 Marcus Streets, Thales e-Security
436 Satish Sundar, IBM
437 Kiran Thota, VMware
438 Somanchi Trinath, Freescale Semiconductor, Inc.
439 Nathan Turajski, Thales e-Security
440 Sean Turner, IECA, Inc.
441 Paul Turner, Venafi, Inc.
442 Rod Wideman, Quantum Corporation
443 Steven Wierenga, Hewlett-Packard
444 Jin Wong, QuintessenceLabs
445 Sameer Yami, Thales e-Security
446 Peter Yee, EMC Corporation
447 Krishna Yellepeddy, IBM
448 Catherine Ying, SafeNet, Inc.
449 Tatu Ylonen, SSH Communications Security (Tectia Corp)

450 Michael Yoder, Vormetric. Inc.
451 Magda Zdunkiewicz, Cryptsoft
452 Peter Zelechowski, Election Systems & Software

Appendix B. Revision History

Revision	Date	Editor	Changes Made
wd01	23-May-2013	Tim Hudson	Initial revision based on the KMIP 1.1 equivalent document and TC discussions
wd02	25-June-2013	Tim Hudson	Removed comments, updated participant list, included line numbers.
pr01update	11-June-2014	Tim Hudson	Updated following Public Review