

# Key Management Interoperability Protocol Profiles Version 1.2

## Committee Specification Draft 01 / Public Review Draft 01

13 March 2014

### Specification URIs

#### This 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>

#### Previous version:

N/A

#### 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:

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

#### Editors:

Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)), Cryptsoft Pty Ltd.  
Robert Lockhart ([Robert.Lockhart@thalessec.com](mailto: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. 13 March 2014. OASIS Committee Specification Draft 01 / Public Review Draft 01. <http://docs.oasis-open.org/kmip/profiles/v1.2/csprd01/kmip-profiles-v1.2-csprd01.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	Object Owner.....	9
3.1.5	KMIP Port Number.....	10
3.2	TLS 1.2 Authentication Suite.....	10
3.2.1	Protocols.....	10
3.2.2	Cipher Suites.....	10
3.2.3	Client Authenticity.....	10
3.2.4	Object Owner.....	10
3.2.5	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]). Illustrative guidance for the implementation of KMIP clients and servers is provided in the KMIP Usage Guide ([KMIP-UG]) and KMIP Test Cases ([KMIP-TC]).

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

## 1.3 Non-Normative References

- [KMIP-UG] [Key Management Interoperability Protocol Usage Guide Version 1.2. DD MMM 2013. OASIS Committee Note 01. URL.](#)
- [KMIP-TC] [Key Management Interoperability Protocol Test Cases Version 1.3. DD MMM 2013. OASIS Committee Note 01. URL.](#)
- [TC-PROC] OASIS TC Process. 14 February 2013. OASIS Process. <https://www.oasis-open.org/policies-guidelines/tc-process>.

---

## 43 2 Profiles

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

### 46 2.1 Guidelines for Specifying Conformance Clauses

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

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

### 54 2.2 Guidelines for Specifying Authentication Suites

- 55 1. Channel Security – For all operations, communication between client and server SHALL  
56 establish and maintain channel confidentiality and integrity,.
- 57 2. Channel Options – Options like protocol version and cipher suite
- 58 3. Server and Client Authenticity – For all operations, communication between client and server  
59 SHALL provide assurance of server authenticity and client authenticity

### 60 2.3 Guidelines for Specifying KMIP Profiles

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

- 62 1. The profile SHALL be publicly available.
- 63 2. The KMIP Technical Committee SHALL be formally advised of the availability of the profile and  
64 the location of the published profile.
- 65 3. The profile SHALL be defined as a tuple of {Conformance Clause, Authentication Suite}.
- 66 4. The KMIP Technical Committee SHOULD review the profile prior to publication.

### 67 2.4 Guidelines for Validating Conformance to KMIP Server Profiles

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

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

### 75 2.5 Guidelines for Validating Conformance to KMIP Client Profiles

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

- 78 1. All objects specified as required in that profile
- 79 2. All operations specified as required in that profile
- 80 3. All attributes specified as required in that profile
- 81 4. The defined wire protocols (TLS, SSL, IPSec, etc...) for that profile
- 82 5. The defined methods of authentication for that profile
- 83

---

## 84 3 Authentication Suites

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

### 87 3.1 Basic Authentication Suite

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

#### 90 3.1.1 Protocols

91 Conformant KMIP clients or servers SHALL support:

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

93 Conformant KMIP clients or servers MAY support:

- 94 • TLS v1.1 [RFC4346]
- 95 • TLS v1.2 [RFC5246]

96 Conformant KMIP clients or servers SHALL NOT support:

- 97 • SSL v3.0
- 98 • SSL v2.0
- 99 • SSL v1.0

#### 100 3.1.2 Cipher Suites

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

- 102 • TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

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

- 104 • TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- 105 • TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- 106 • TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- 107 • TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- 108 • TLS\_DH\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA
- 109 • TLS\_DH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- 110 • TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA
- 111 • TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- 112 • TLS\_DH\_DSS\_WITH\_AES\_128\_CBC\_SHA
- 113 • TLS\_DH\_RSA\_WITH\_AES\_128\_CBC\_SHA
- 114 • TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA
- 115 • TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- 116 • TLS\_DH\_DSS\_WITH\_AES\_256\_CBC\_SHA
- 117 • TLS\_DH\_RSA\_WITH\_AES\_256\_CBC\_SHA
- 118 • TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA
- 119 • TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- 120 • TLS\_DH\_DSS\_WITH\_AES\_128\_CBC\_SHA256
- 121 • TLS\_DH\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- 122 • TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256
- 123 • TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- 124 • TLS\_DH\_DSS\_WITH\_AES\_256\_CBC\_SHA256
- 125 • TLS\_DH\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- 126 • TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256



- 127 • TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- 128 • TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA
- 129 • TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA
- 130 • TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- 131 • TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384
- 132 • TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA
- 133 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA
- 134 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- 135 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384
- 136 • TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- 137 • TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- 138 • TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- 139 • TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- 140 • TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- 141 • TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- 142 • TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- 143 • TLS\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA
- 144 • TLS\_PSK\_WITH\_AES\_128\_CBC\_SHA
- 145 • TLS\_PSK\_WITH\_AES\_256\_CBC\_SHA
- 146 • TLS\_DHE\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA
- 147 • TLS\_DHE\_PSK\_WITH\_AES\_128\_CBC\_SHA
- 148 • TLS\_DHE\_PSK\_WITH\_AES\_256\_CBC\_SHA
- 149 • TLS\_RSA\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA
- 150 • TLS\_RSA\_PSK\_WITH\_AES\_128\_CBC\_SHA
- 151 • TLS\_RSA\_PSK\_WITH\_AES\_256\_CBC\_SHA
- 152 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- 153 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- 154 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- 155 • TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384

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

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

### 159 3.1.3 Client Authenticity

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

- 162 • Query
- 163 • Discover Versions

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

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

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

### 170 3.1.4 Object Owner

171 Conformant KMIP servers SHALL use the client identity as the owner (or creator) of any new managed  
 172 objects created as the result of a KMIP client request.

173 Conformant KMIP servers SHALL evaluate allowed operations and access to existing managed objects  
 174 as mandated by section 3.18 (Operation Policy Name) of [KMIP-SPEC].

175 **3.1.5 KMIP Port Number**

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

177 **3.2 TLS 1.2 Authentication Suite**

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

180 **3.2.1 Protocols**

181 Conformant KMIP clients and servers SHALL support:

- 182
  - TLS v1.2 [RFC2246]

183 **3.2.2 Cipher Suites**

184 Conformant KMIP servers SHALL support the following cipher suites:

- 185
  - TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256
  - TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

187

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

190 **3.2.3 Client Authenticity**

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

193 **3.2.4 Object Owner**

194 Conformant KMIP servers and clients SHALL handle object owner in accordance with section 3.2.3 of the  
195 Basic Authentication Suite.

196 **3.2.5 KMIP Port Number**

197 Conformant KMIP servers and clients SHALL handle the KMIP port number in accordance with section  
198 3.1.5 of the Basic Authentication Suite.

---

## 199 **4 KMIP Profiles**

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

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

### 203 **4.1 Baseline Server Basic KMIP Profile**

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

### 205 **4.2 Baseline Server TLS v1.2 KMIP Profile**

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

### 207 **4.3 Baseline Client Basic KMIP Profile**

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

### 209 **4.4 Baseline Client TLS v1.2 KMIP Profile**

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

### 211 **4.5 Complete Server Basic KMIP Profile**

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

### 213 **4.6 Complete Server TLS v1.2 KMIP Profile**

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

215

---

## 216 5 Conformance

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

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

### 224 5.1 Baseline Server

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

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

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

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

## 291 5.2 Baseline Client

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

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

- 295 1. Supports the conditions required by the KMIP Client conformance clauses ([KMIP-SPEC] 12.2)
- 296 2. Supports the following objects:
  - 297 a. Attribute ([KMIP-SPEC] 2.1.1)
  - 298 b. Template-Attribute Structure ([KMIP-SPEC] 2.1.8)
- 299 3. Supports the following subsets of attributes:
  - 300 a. Unique Identifier ([KMIP-SPEC] 3.1)
  - 301 b. Object Type ([KMIP-SPEC] 3.3)
  - 302 c. Digest ([KMIP-SPEC] 3.17)
  - 303 d. Default Operation Policy ([KMIP-SPEC] 3.18.2)
  - 304 e. State ([KMIP-SPEC] 3.22)
  - 305 f. Initial Date ([KMIP-SPEC] 3.23)
  - 306 g. Activation Date ([KMIP-SPEC] 3.24)
  - 307 h. Deactivation Date ([KMIP-SPEC] 3.27)
  - 308 i. Last Change Date ([KMIP-SPEC] 3.38)
- 309 4. Supports the ID Placeholder ([KMIP-SPEC] 4)
- 310 5. Supports the following client-to-server operations:
  - 311 a. Locate ([KMIP-SPEC] 4.9)
  - 312 b. Get ([KMIP-SPEC] 4.11)

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

### 336 5.3 Complete Server

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

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

- 340 1. Supports KMIP Server conformance clauses ([KMIP-SPEC] 12.1)
- 341 2. Supports Objects ([KMIP-SPEC] 2)
- 342 3. Supports Attributes ([KMIP-SPEC] 3)
- 343 4. Supports Client-to-Server operations ([KMIP-SPEC] 4)
- 344 5. Supports Server-to-Client operations ([KMIP-SPEC] 5)
- 345 6. Supports Message Contents ([KMIP-SPEC] 6)
- 346 7. Supports Message Formats ([KMIP-SPEC] 7)
- 347 8. Supports Authentication ([KMIP-SPEC] 8)
- 348 9. Supports Message Encodings ([KMIP-SPEC] 9)
- 349 10. Supports Error Handling ([KMIP-SPEC] 11)
- 350 11. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions,
- 351 conformance clauses) that do not contradict any KMIP requirements

352

---

## Appendix A. Acknowledgments

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

356 **Participants:**

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

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



463 Michael Yoder, Vormetric. Inc.  
464 Magda Zdunkiewicz, Cryptsoft  
465 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.