



# Key Management Interoperability Protocol Profiles Version 1.0

## Committee Specification 01

15 June 2010

### Specification URIs:

#### This Version:

<http://docs.oasis-open.org/kmip/profiles/v1.0/cs01/kmip-profiles-1.0-cs-01.html>  
<http://docs.oasis-open.org/kmip/profiles/v1.0/cs01/kmip-profiles-1.0-cs-01.doc> (Authoritative)  
<http://docs.oasis-open.org/kmip/profiles/v1.0/cs01/kmip-profiles-1.0-cs-01.pdf>

#### Previous Version:

<http://docs.oasis-open.org/kmip/profiles/v1.0/cd06/kmip-profiles-1.0-cd-06.html>  
<http://docs.oasis-open.org/kmip/profiles/v1.0/cd06/kmip-profiles-1.0-cd-06.doc> (Authoritative)  
<http://docs.oasis-open.org/kmip/profiles/v1.0/cd06/kmip-profiles-1.0-cd-06.pdf>

#### Latest Version:

<http://docs.oasis-open.org/kmip/profiles/v1.0/kmip-profiles-1.0.html>  
<http://docs.oasis-open.org/kmip/profiles/v1.0/kmip-profiles-1.0.doc>  
<http://docs.oasis-open.org/kmip/profiles/v1.0/kmip-profiles-1.0.pdf>

### Technical Committee:

OASIS Key Management Interoperability Protocol (KMIP) TC

### Chair(s):

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

### Editor(s):

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

### Related work:

This specification replaces or supersedes:

- None

This specification is related to:

- [Key Management Interoperability Protocol Specification v1.0](#)
- [Key Management Interoperability Protocol Use Cases v1.0](#)
- [Key Management Interoperability Protocol Usage Guide v1.0](#)

### Declared XML Namespace(s):

None

### Abstract:

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

### Status:

This document was last revised or approved by the Key Management Interoperability Protocol TC on the above date. The level of approval is also listed above. Check the “Latest Version” or “Latest Approved 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>).

The non-normative errata page for this specification is located at <http://www.oasis-open.org/committees/kmip/>.

---

## Notices

Copyright © OASIS® 2010. 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 names "OASIS", "KMIP" are trademarks 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/who/trademark.php> 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.....	7
2.1	Guidelines for Specifying Conformance Clauses .....	7
2.2	Guidelines for Specifying Authentication Suites .....	7
2.3	Guidelines for Specifying KMIP Profiles .....	7
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 .....	8
3.1.4	Object Creator.....	8
3.2	TLS 1.2 Authentication Suite .....	9
3.2.1	Protocols .....	9
3.2.2	Cipher Suites.....	9
3.2.3	Client Authenticity .....	9
3.2.4	Object Creator.....	9
4	KMIP Profiles.....	10
4.1	Secret Data KMIP Profile.....	10
4.2	Basic Symmetric Key Store and Server KMIP Profile.....	10
4.3	Basic Symmetric Key Foundry and Server KMIP Profile .....	10
4.4	Secret Data TLS 1.2 Authentication KMIP Profile .....	10
4.5	Basic Symmetric Key Store and Server TLS 1.2 Authentication KMIP Profile.....	10
4.6	Basic Symmetric Key Foundry and Server TLS 1.2 Authentication KMIP Profile .....	10
5	Conformance Clauses .....	11
5.1	Secret Data Server Clause.....	11
5.1.1	Implementation Conformance .....	11
5.1.2	Conformance of a Secret Data Server .....	11
5.2	Basic Symmetric Key Store and Server Conformance Clause .....	11
5.2.1	Implementation Conformance .....	11
5.2.2	Conformance as a Basic Symmetric Key Store and Server .....	12
5.3	Basic Symmetric Key Foundry and Server Conformance Clause .....	12
5.3.1	Implementation Conformance .....	12
5.3.2	Conformance as a KMIP Basic Symmetric Key Foundry and Server .....	12
A.	Acknowledgements .....	14
B.	Revision History.....	16

---

# 1 Introduction

OASIS requires a conformance section in an approved committee specification (see [TCProc], section 2.18 Specification Quality):

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 ([KMIP-Spec] 12.1) 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](#). Illustrative guidance for the implementation of KMIP clients and servers is provided in the [KMIP Usage Guide](#).

## 1.1 Terminology

The key words "SHALL", "SHALL NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]. The words 'must', 'can', and 'will' are forbidden.

For definitions not found in this document, see [KMIP-Spec] definitions **Error! Reference source not found.**

## 1.2 Normative References

- [RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.
- [KMIP-Spec] OASIS Committee Specification 01, Key Management Interoperability Protocol Specification Version 1.0, June 2010, <http://docs.oasis-open.org/kmip/spec/v1.0/cs01/kmip-spec-1.0-cs-01.doc>
- [RFC 2246] T. Dierks & C.Allen, The TLS Protocol, Version 1.0, <http://www.ietf.org/rfc/rfc2246.txt>, IETF RFC 2246, January 1999
- [RFC 3268] P. Chown, Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), <http://www.ietf.org/rfc/rfc3268.txt>, IETF RFC 3268, June 2002
- [RFC 4346] 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
- [RFC 5246] 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
- [NIST 800-57 Part 3] Barker, Burr, et.al, Recommendation for Key Management Part 3: Application-Specific Key Management Guidance, [http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57\\_PART3\\_key-management\\_Dec2009.pdf](http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf), December 2009

## 1.3 Non-normative References

- [KMIP-UG] OASIS Committee Specification 01, Key Management Interoperability Protocol Usage Guide Version 1.0, June 2010, <http://docs.oasis-open.org/kmip/ug/v1.0/cs01/kmip-ug-1.0-cs-01.doc>

46  
47  
48

**[KMIP-UC]**

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

---

## 49 2 Profiles

50 This document defines a selected set of conformance clauses and authentication suites which when  
51 “paired together” form KMIP Profiles. The KMIP TC also welcomes proposals for new profiles. KMIP TC  
52 members are encouraged to submit these proposals to the KMIP TC for consideration for inclusion in a  
53 future version of this TC-approved document. However, some OASIS members may simply wish to inform  
54 the committee of profiles or other work related to KMIP.

### 55 2.1 Guidelines for Specifying Conformance Clauses

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

- 57 1. Implement functionality as mandated by Section 12.1 (Conformance clauses for a KMIP servers)
- 58 2. Specify the list of additional objects that SHALL be supported
- 59 3. Specify the list of additional attributes that SHALL be supported
- 60 4. Specify the list of additional operations that SHALL be supported
- 61 5. Specify any additional message content that SHALL be supported

### 62 2.2 Guidelines for Specifying Authentication Suites

- 63 1. Channel Security – Client to Server communication SHALL establish and maintain channel  
64 confidentiality and integrity, and provide assurance of server authenticity
- 65 2. Channel Options – Options like protocol version and cipher suite
- 66 3. Client Authenticity – The options that are used to provide assurance of client authenticity

### 67 2.3 Guidelines for Specifying KMIP Profiles

68 A KMIP profile is a tuple of {Conformance Clause, Authentication Suite}

---

## 69 3 Authentication suites

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

### 72 3.1 Basic Authentication Suite

73 This authentication set stipulates that a KMIP client and server SHALL use TLS to negotiate a mutually-  
74 authenticated connection with the exception of the Query operation. The query operation SHALL NOT  
75 require the client to provide assurance of its authenticity.

#### 76 3.1.1 Protocols

77 Conformant KMIP servers SHALL support TLSv1.0. They MAY support TLS v1.1 [RFC 4346], TLS v1.2  
78 [RFC 5246] bearing in mind that they are not compatible with each other and SHALL NOT support  
79 SSLv3.0, SSLv2.0 and SSLv1.0.

#### 80 3.1.2 Cipher Suites

81 Conformant KMIP servers SHALL support the following cipher suites:

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

83 Basic Authentication Suite Conformant KMIP servers MAY support the cipher suites listed in tables 4-1  
84 through 4-4 of NIST 800-57 Part 3 with the exception of NULL ciphers (at the time this document was  
85 created, the only NULL cipher in 800-57 Part 3 was: TLS\_RSA\_WITH\_NONE\_SHA)

86 Basic Authentication Suite Conformant KMIP servers SHALL NOT support any other cipher suites.

87 NOTE: TLS 1.0 has some security issues as described in <http://www.openssl.org/~bodo/tls-cbc.txt>.  
88 Implementations that need protections against this attack should considering using the “TLS 1.2  
89 Authentication Suite”

90 *At the time this document was published, NIST 800-57 Part 3 Table 4-1, for cipher suites that have both*  
91 *SHA1 and SHA256 variants, erroneously categorizes SHA256 based ciphers under TLS versions 1.0, 1.1*  
92 *and 1.2 and SHA1 based ciphers under TLS 1.2. The correct value for SHA256 based ciphers should 1.2*  
93 *and for SHA1 based ciphers it should be 1.0, 1.2 and 1.2.*

#### 94 3.1.3 Client Authenticity

95 For authenticated services (all operations save Query) KMIP servers SHALL require the use of channel  
96 (TLS) mutual authentication to provide assurance of client authenticity.

97  
98 In the absence of Credential information in the request header, KMIP servers SHALL use the identity  
99 derived from the channel authentication as the client identity.

100  
101 In the presence of Credential information in the request header, KMIP servers SHALL consider such  
102 Credential information into their evaluation of client authenticity and identity, along with the authenticity  
103 and identity derived from the channel. The exact mechanisms for such evaluation are outside the scope  
104 of this specification.

#### 105 3.1.4 Object Creator

106 KMIP objects have a `creator`. For those KMIP requests that result in new managed objects the client  
107 identity SHALL be used as the creator of the managed object. For those operations that only access pre-  
108 existent managed objects, the client identity SHALL be checked against the creator and access SHALL  
109 be controlled as detailed in section 3.13 of [KMIP].



## 110 **3.2 TLS 1.2 Authentication Suite**

111 This authentication set stipulates that a KMIP client and server SHALL use TLS to negotiate a mutually-  
112 authenticated connection with the exception of the Query operation. The query operation SHALL NOT  
113 require the client to provide assurance of its authenticity.

### 114 **3.2.1 Protocols**

115 Conformant KMIP servers SHALL support TLSv1.2

### 116 **3.2.2 Cipher Suites**

117 Conformant KMIP servers SHALL support the following cipher suites:

- 118 • TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- 119 • TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256

120 TLS 1.2 Authentication Suite Conformant KMIP servers MAY support the cipher suites listed in tables 4-1  
121 through 4-4 of NIST 800-57 Part 3 with the exception of NULL ciphers (at the time this document was  
122 created, the only NULL cipher in 800-57 Part 3 was: TLS\_RSA\_WITH\_NONE\_SHA)

123 TLS 1.2 Authentication Suite Conformant KMIP servers SHALL NOT support any other cipher suites

124 *NIST 800-57 Part 3 Table 4-1, for cipher suites that have both SHA1 and SHA256 variants, erroneously*  
125 *categorizes SHA256 based ciphers under TLS versions 1.0, 1.1 and 1.2 and SHA1 based ciphers under*  
126 *TLS 1.2. The correct value for SHA256 based ciphers should be 1.2 and for SHA1 based ciphers it should*  
127 *be 1.0, 1.2 and 1.2.*

### 128 **3.2.3 Client Authenticity**

129 Same as the basic authentication suite (See Section 3.1.3)

### 130 **3.2.4 Object Creator**

131 Same as the basic authentication suite (See Section 3.1.4)

---

## 132 4 KMIP Profiles

133 This section lists the KMIP profiles that are defined in this specification. More than one profile may be  
134 supported at the same time provided there are no conflicting requirements.

### 135 4.1 Secret Data KMIP Profile

136 A profile that consists of the tuple {Secret Data Server Conformance Clause, Basic Authentication Suite}

### 137 4.2 Basic Symmetric Key Store and Server KMIP Profile

138 A profile that consists of the tuple {Basic Symmetric Key Store and Server Conformance Clause, Basic  
139 Authentication Suite}

### 140 4.3 Basic Symmetric Key Foundry and Server KMIP Profile

141 A profile that consists of the tuple {Basic Symmetric Key Foundry and Server Conformance Clause, Basic  
142 Authentication Suite}

### 143 4.4 Secret Data TLS 1.2 Authentication KMIP Profile

144 A profile that consists of the tuple {Secret Data Server Conformance Clause, TLS 1.2 Authentication  
145 Suite}

### 146 4.5 Basic Symmetric Key Store and Server TLS 1.2 Authentication 147 KMIP Profile

148 A profile that consists of the tuple {Basic Symmetric Key Store and Server Conformance Clause, TLS 1.2  
149 Authentication Suite}

### 150 4.6 Basic Symmetric Key Foundry and Server TLS 1.2 151 Authentication KMIP Profile

152 A profile that consists of the tuple {Basic Symmetric Key Foundry and Server Conformance Clause, TLS  
153 1.2 Authentication Suite}

154

---

## 155 5 Conformance Clauses

156 The following subsections describe currently-defined profiles related to the use of KMIP in support of  
157 secret data and symmetric key operations.

### 158 5.1 Secret Data Server Clause

159 This proposal builds on the KMIP server conformance clauses to provide some of the most basic  
160 functionality that would be expected of a conformant KMIP server – the ability to create, register and get  
161 secret data in an interoperable fashion.

#### 162 5.1.1 Implementation Conformance

163 An implementation is a conforming Secret Data Server Clause if it meets the conditions as outlined in the  
164 following section.

#### 165 5.1.2 Conformance of a Secret Data Server

166 An implementation conforms to this specification as a Secret Data Server if it meets the following  
167 conditions:

- 168 1. Supports the conditions required by the KMIP Server conformance clauses ([KMIP-Spec] 12.1)
- 169 2. Supports the following additional objects:
  - 170 a. Secret Data ([KMIP-Spec] 2.2.7)
- 171 3. Supports the following client-to-server operations:
  - 172 a. Register ([KMIP-Spec] 4.3)
- 173 4. Supports the following subsets of enumerated attributes:
  - 174 a. Object Type ([KMIP-Spec] 3.3 and 9.1.3.2.11)
    - 175 i. Secret Data
  - 176 b. Secret Data Type ([KMIP-Spec] 9.1.3.2.8)
    - 177 i. Password
- 178 5. Supports the following subsets of enumerated objects (see clauses 3 and 9):
  - 179 a. Key Format Type ([KMIP-Spec] 9.1.3.2.3)
    - 180 i. Opaque
- 181 6. Optionally supports any clause within [KMIP-Spec] specification that is not listed above
- 182 7. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions,  
183 conformance clauses) that do not contradict any KMIP requirements

### 184 5.2 Basic Symmetric Key Store and Server Conformance Clause

185 This proposal builds on the KMIP server conformance clauses to provide support for symmetric key store  
186 and foundry use cases.

#### 187 5.2.1 Implementation Conformance

188 An implementation is a conforming KMIP Basic Symmetric Key Store and Server if the implementation  
189 meets the conditions as outlined in the following section.

## 190 5.2.2 Conformance as a Basic Symmetric Key Store and Server

191 An implementation conforms to this specification as a Basic Symmetric Key Store and Server if it meets  
192 the following conditions:

- 193 1. Supports the conditions required by the KMIP Server conformance clauses. ([KMIP-Spec] 12.1)
- 194 2. Supports the following additional objects:
  - 195 a. Symmetric Key ([KMIP-Spec] 2.2.2)
- 196 3. Supports the following client-to-server operations:
  - 197 a. Register ([KMIP-Spec] 4.3)
- 198 4. Supports the following attributes:
  - 199 a. Process Start Date ([KMIP-Spec] 3.20)
  - 200 b. Protect Stop Date ([KMIP-Spec] 3.21)
- 201 5. Supports the following subsets of enumerated attributes:
  - 202 a. Cryptographic Algorithm ([KMIP-Spec] 3.4 and 9.1.3.2.12)
    - 203 i. 3DES
    - 204 ii. AES
  - 205 b. Object Type ([KMIP-Spec] 3.3 and 9.1.3.2.11)
    - 206 i. Symmetric Key
- 207 6. Supports the following subsets of enumerated objects:
  - 208 a. Key Format Type ([KMIP-Spec] 3.4 and 9.1.3.2.3)
    - 209 i. Raw
    - 210 ii. Transparent Symmetric Key
- 211 7. Optionally supports any clause within [KMIP-Spec] specification that is not listed above
- 212 8. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions,  
213 conformance clauses) that do not contradict any KMIP requirements

## 214 5.3 Basic Symmetric Key Foundry and Server Conformance Clause

215 This proposal intends to meet this OASIS requirement by building on the KMIP Server Conformance  
216 Clause defined in the KMIP Specification to provide basic symmetric key services. The intent is to simply  
217 allow key creation and serving with very limited key types.

### 218 5.3.1 Implementation Conformance

219 An implementation is a conforming KMIP Basic Symmetric Key Store and Server if the implementation  
220 meets the conditions as outlined in the following section.

### 221 5.3.2 Conformance as a KMIP Basic Symmetric Key Foundry and Server

222 An implementation conforms to this specification as a KMIP Basic Symmetric Key Foundry and Server if it  
223 meets the following conditions:

- 224 1. Supports the conditions required by the KMIP Server conformance clauses. ([KMIP-Spec] 12.1)
- 225 2. Supports the following additional objects
  - 226 a. Symmetric Key ([KMIP-Spec] 2.2.2)
- 227 3. Supports the following client-to-server operations:
  - 228 a. Create ([KMIP-Spec] 4.1)
- 229 4. Supports the following attributes:
  - 230 a. Process Start Date ([KMIP-Spec] 3.20)

- 231                   b. Protect Stop Date (**[KMIP-Spec]** 3.21)
- 232           5. Supports the following subsets of enumerated attributes:
- 233            a. Cryptographic Algorithm (**[KMIP-Spec]** 3.4 and 9.1.3.2.12)
- 234                i. 3DES
- 235                ii. AES
- 236            b. Object Type (**[KMIP-Spec]** 3.3 and 9.1.3.2.11)
- 237                i. Symmetric Key
- 238           6. Supports the following subsets of enumerated objects:
- 239            a. Key Format Type (**[KMIP-Spec]** 3.4 and 9.1.3.2.3)
- 240                i. Raw
- 241                ii. Transparent Symmetric Key
- 242           7. Optionally supports any clause within **[KMIP-Spec]** specification that is not listed above
- 243           8. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions,
- 244            conformance clauses) that do not contradict any KMIP requirements
- 245
- 246

---

## 247 A. Acknowledgements

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

### 250 **Original Authors of the initial contribution:**

251 Bruce Rich, IBM

### 252 **Participants:**

253  
254  
255 Mike Allen, PGP Corporation  
256 Gordon Arnold, IBM  
257 Todd Arnold, IBM  
258 Matthew Ball, Oracle Corporation  
259 Elaine Barker, NIST  
260 Peter Bartok, Venafi, Inc.  
261 Mathias Björkqvist, IBM  
262 Kevin Bocek, Thales e-Security  
263 Kelley Burgin, National Security Agency  
264 Jon Callas, PGP Corporation  
265 Tom Clifford, Symantec Corp.  
266 Graydon Dodson, Lexmark International Inc.  
267 Chris Dunn, SafeNet, Inc.  
268 Paul Earsy, SafeNet, Inc.  
269 Stan Feather, Hewlett-Packard  
270 Indra Fitzgerald, Hewlett-Packard  
271 Alan Frindell, SafeNet, Inc.  
272 Judith Furlong, EMC Corporation  
273 Jonathan Geater, Thales e-Security  
274 Robert Griffin, EMC Corporation  
275 Robert Haas, IBM  
276 Thomas Hardjono, M.I.T.  
277 Kurt Heberlein, 3PAR, Inc.  
278 Marc Hocking, BeCrypt Ltd.  
279 Larry Hofer, Emulex Corporation  
280 Brandon Hoff, Emulex Corporation  
281 Walt Hubis, LSI Corporation  
282 Tim Hudson, Cryptsoft Pty Ltd.  
283 Wyllys Ingersoll, Oracle Corporation  
284 Jay Jacobs, Target Corporation  
285 Glen Jaquette, IBM  
286 Scott Kipp, Brocade Communications Systems, Inc.  
287 David Lawson, Emulex Corporation  
288 Hal Lockhart, Oracle Corporation  
289 Robert Lockhart, Thales e-Security  
290 Shyam Mankala, EMC Corporation  
291 Upendra Mardikar, PayPal Inc.  
292 Marc Massar, Individual  
293 Don McAlister, Associate  
294 Hyrum Mills, Mitre Corporation  
295 Bob Nixon, Emulex Corporation  
296 Landon Curt Noll, Cisco Systems, Inc.  
297 René Pawlitzek, IBM  
298 John Peck, IBM  
299 Rob Philpott, EMC Corporation

300 Scott Rea, Individual  
301 Bruce Rich, IBM  
302 Scott Rotondo, Oracle Corporation  
303 Saikat Saha, Vormetric, Inc.  
304 Anil Saldhana, Red Hat  
305 Subhash Sankuratripati, NetApp  
306 Mark Schiller, Hewlett-Packard  
307 Jitendra Singh, Brocade Communications Systems, Inc.  
308 Servesh Singh, EMC Corporation  
309 Terence Spies, Voltage Security  
310 Sandy Stewart, Oracle Corporation  
311 Marcus Streets, Thales e-Security  
312 Brett Thompson, SafeNet, Inc.  
313 Benjamin Tomhave, Individual  
314 Sean Turner, IECA, Inc.  
315 Paul Turner, Venafi, Inc.  
316 Marko Vukolić, IBM  
317 Rod Wideman, Quantum Corporation  
318 Steven Wierenga, Hewlett-Packard  
319 Peter Yee, EMC Corporation  
320 Krishna Yellepeddy, IBM  
321 Peter Zelechowski, Election Systems & Software  
322 Grace Zhang, Skyworth TTG Holdings Limited

## B. Revision History

Revision	Date	Editor	Changes Made
ed-0.98	2009-09-18	Robert Griffin	Initial conversion of symmetric key profiles, as created by Bruce Rich, into this KMIP Profiles document.
ed-0.98	2009-09-29	Subhash Sankuratripati	Adding the notion of authentication sets
ed-0.99	2009-10-05	Subhash Sankuratripati	Incorporating feedback that was received during the F2F
ed-0.99	2009-10-21	Subhash Sankuratripati	Incorporating additional feedback and getting the document ready to be committee draft
ed-0.99	2009-10-23	Subhash Sankuratripati	Other minor edits
ed-0.99	2009-11-01	Subhash Sankuratripati	More editorial changes
ed-0.99	2009-11-06	Subhash Sankuratripati	Version that is to be submitted as committee draft
cd-01	2009-11-06	Subhash Sankuratripati	First version as committee draft
cd-02	2009-11-09	Subhash Sankuratripati	Corrected reference to conformance clause section of [KMIP-Spec] from 13.1 to 12.1 and another minor edit.
cd-03	2009-11-11	Subhash Sankuratripati	Accepting all changes and removing previous versions
cd-04	2010-11-12	Subhash Sankuratripati	Corrected document URIs
cd-05	2010-03-05	Subhash Sankuratripati	Addressing public review comments by adding <ul style="list-style-type: none"> <li>- Support for TLS 1.2,</li> <li>- Adding references to normative documents</li> <li>- Added an informative warning regarding the usage of TLS 1.0 in certain scenarios due to a security issue</li> <li>- Added an errata for NIST 800-57 Part 3</li> </ul>
cd-06	2010-05-26	Subhash Sankuratripati	Updating references to latest committee draft versions and participant list