Key Management Interoperability Protocol Profiles Version 1.0

Committee Draft 04 / Public Review 01

5 November 2009

Specification URIs:
This Version:
http://docs.oasis-open.org/kmip/profiles/v1.0/cd04/kmip-profiles-1.0-cd-04.html
http://docs.oasis-open.org/kmip/profiles/v1.0/cd04/kmip-profiles-1.0-cd-04.doc (Authoritative)
http://docs.oasis-open.org/kmip/profiles/v1.0/cd04/kmip-profiles-1.0-cd-04.pdf

Previous Version:
N/A

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>
Subhash Sankuratripati, NetApp <Subhash.Sankuratripati@netapp.com>

Editor(s):
Robert Griffin, EMC Corporation <robert.griffin@rsa.com>
Subhash Sankuratripati, NetApp <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

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

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 **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 Draft 06, *Key Management Interoperability Protocol Specification v1,0,* November 2009. http://docs.oasis-open.org/kmip/spec/v1.0/cd06/kmip-spec-1.0-cd-06.doc

1.3 Non-normative References

[KMIP-UG] OASIS Committee Draft 05, *Key Management Interoperability Protocol Usage Guide v1.0*, November 2009. http://docs.oasis-open.org/kmip/ug/v1.0/cd05/kmip-ug-1.0-cd-05.doc

[KMIP-UC] OASIS Committee Draft 05, *Key Management Interoperability Protocol Use Cases v1.0,* November 2009. http://docs.oasis-open.org/kmip/usecases/v1.0/cd05/kmip-usecases-1.0-cd-05.doc

2 Profiles

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

2.1 Guidelines for Specifying Conformance Clauses

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

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

2.2 Guidelines for Specifying Authentication Suites

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

2.3 Guidelines for Specifying KMIP Profiles

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

3 Authentication suites

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

3.1 Basic Authentication Suite

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

3.1.1 Protocols

Conformant KMIP servers SHALL support SSLv3.1 and TLSv1.0. They MAY support TLS v1.1 [RFC 4346], TLS v1.2 [RFC 5246] but SHALL NOT support SSLv3.0, SSLv2.0 and SSLv1.0.

3.1.2 Cipher Suites

Conformant KMIP servers SHALL support the following cipher suites:

- A TLSv1.0-capable instance SHALL support `TLS_RSA_WITH_AES_128_CBC_SHA`
- An SSLv3.1-capable instance SHALL support `SSL_RSA_WITH_AES_128_CBC_SHA`

Basic Authentication Suite Conformant KMIP servers MAY support the cipher suites listed in tables 4-1 through 4-4 of NIST 800-57 Part 3 with the exception of NULL ciphers (at the time this document was created, the only NULL cipher in 800-57 Part 3 was: `TLS_RSA_WITH_NONE_SHA`)

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

NOTE: 800-57 does not distinguish between TLS vs. SSL. SSLv3.1 can be substituted for TLS in the Cipher Suite strings.

3.1.3 Client Authenticity

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

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

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

3.1.4 Object Creator

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

4 KMIP Profiles

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

4.1 Secret Data KMIP Profile

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

4.2 Basic Symmetric Key Store and Server KMIP Profile

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

4.3 Basic Symmetric Key Foundry and Server KMIP Profile

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

5 Conformance Clauses

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

5.1 Secret Data Server Clause

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

5.1.1 Implementation Conformance

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

5.1.2 Conformance of a Secret Data Server

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

1. Supports the conditions required by the KMIP Server conformance clauses (**[KMIP-Spec]** 12.1)
2. Supports the following additional objects:
    a. Secret Data (**[KMIP-Spec]** 2.2.7)
3. Supports the following client-to-server operations:
    a. Register (**[KMIP-Spec]** 4.3)
4. As listed in the KMIP server conformance clauses (**[KMIP-Spec]** 12.1)
5. Supports the following subsets of enumerated attributes:
    a. Object Type (**[KMIP-Spec]** 3.3 and 9.1.3.2.11)
        i. Secret Data
    b. Secret Data Type (**[KMIP-Spec]** 9.1.3.2.8)
        i. Password
6. Supports the following subsets of enumerated objects (see clauses 3 and 9):
    a. Key Format Type (**[KMIP-Spec]** 9.1.3.2.3)
        i. Raw
7. Optionally supports any clause within **[KMIP-Spec]** specification that is not listed above
8. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions, conformance clauses) that do not contradict any KMIP requirements

5.2 Basic Symmetric Key Store and Server Conformance Clause

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

5.2.1 Implementation Conformance

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

5.2.2 Conformance as a Basic Symmetric Key Store and Server

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

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

5.3 Basic Symmetric Key Foundry and Server Conformance Clause

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

5.3.1 Implementation Conformance

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

5.3.2 Conformance as a KMIP Basic Symmetric Key Foundry and Server

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

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

b. Protect Stop Date (**[KMIP-Spec]** 3.21)

5. Supports the following subsets of enumerated attributes:
    a. Cryptographic Algorithm (**[KMIP-Spec]** 3.4 and 9.1.3.2.12)
        i. 3DES
        ii. AES
    b. Object Type (**[KMIP-Spec]** 3.3 and 9.1.3.2.11)
        i. Symmetric Key
6. Supports the following subsets of enumerated objects:
    a. Key Format Type (**[KMIP-Spec]** 3.4 and 9.1.3.2.3)
        i. Raw
        ii. Transparent Symmetric Key
7. Optionally supports any clause within **[KMIP-Spec]**specification that is not listed above
8. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions, conformance clauses) that do not contradict any KMIP requirements

A. Acknowledgements

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

Original Authors of the initial contribution:

Bruce Rich, IBM

Participants:

Gordon Arnold, IBM
Todd Arnold, IBM
Matthew Ball, Sun Microsystems
Elaine Barker, NIST
Peter Bartok, Venafi, Inc.
Mathias Bjorkqvist, IBM
Kevin Bocek, Thales e-Security
Kelley Burgin, National Security Agency
Jon Callas, PGP Corporation
Tom Clifford, Symantec Corp.
Graydon Dodson, Lexmark International Inc.
Chris Dunn, SafeNet, Inc.
Paul Earsy, SafeNet, Inc.
Stan Feather, HP
Indra Fitzgerald, HP
Alan Frindell, SafeNet, Inc.
Judith Furlong, EMC Corporation
Jonathan Geater, Thales e-Security
Robert Griffin, EMC Corporation
Robert Haas, IBM
Thomas Hardjono, M.I.T.
Marc Hocking, BeCrypt Ltd.
Larry Hofer, Emulex Corporation
Brandon Hoff, Emulex Corporation
Walt Hubis, LSI Corporation
Wyllys Ingersoll, Sun Microsystems
Jay Jacobs, Target Corporation
Glen Jaquette, IBM
Scott Kipp, Brocade Communications Systems, Inc.
David Lawson, Emulex Corporation
Robert Lockhart, Thales e-Security
Shyam Mankala, EMC Corporation
Marc Massar, Individual
Don McAlister, Associate
Hyrum Mills, Mitre Corporation
Landon Noll, Cisco Systems, Inc.
René Pawlitzek, IBM
Rob Philpott, EMC Corporation
Bruce Rich, IBM
Scott Rotondo, Sun Microsystems
Anil Saldhana, Red Hat
Subhash Sankuratripati, NetApp
Mark Schiller, HP
Jitendra Singh, Brocade Communications Systems, Inc.
Servesh Singh, EMC Corporation
Sandy Stewart, Sun Microsystems

Marcus Streets, Thales e-Security
Brett Thompson, SafeNet, Inc.
Benjamin Tomhave, Individual
Sean Turner, IECA, Inc.
Paul Turner, Venafi, Inc.
Marko Vukolic, IBM
Rod Wideman, Quantum Corporation
Steven Wierenga, HP
Peter Yee, EMC Corporation
Krishna Yellepeddy, IBM
Peter Zelechoski, Associate

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	2009-11-12	Subhash Sankuratripati	Corrected document URIs