# Key Management Interoperability Protocol Profiles Version 2.0

**Key Management Interoperability Protocol Profiles Version 2.0**

**OASIS Standard**

**31 October 2019**

**This version:**

https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/os/kmip-profiles-v2.0-os.docx (Authoritative)

https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/os/kmip-profiles-v2.0-os.html

https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/os/kmip-profiles-v2.0-os.pdf

**Previous version:**

https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/csd01/kmip-profiles-v2.0-csd01.docx

(Authoritative)

https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/csd01/kmip-profiles-v2.0-csd01.html

https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/csd01/kmip-profiles-v2.0-csd01.pdf

**Latest version:**

https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/kmip-profiles-v2.0.docx (Authoritative)

https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/kmip-profiles-v2.0.html

https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/kmip-profiles-v2.0.pdf

**Technical Committee:**

OASIS Key Management Interoperability Protocol (KMIP) TC

**Chairs:**

Tony Cox (tony.cox@cryptsoft.com), Cryptsoft Pty Ltd.

Judith Furlong (Judith.Furlong@dell.com), Dell

**Editors:**

Tim Hudson (tjh@cryptsoft.com), Cryptsoft Pty Ltd.

Robert Lockhart (Robert.Lockhart@thalesesec.com), Thales e-Security

**Additional artifacts:**

This prose specification is one component of a Work Product that also includes:

- Mandatory test cases: https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/os/test-cases/kmip-v2.0/mandatory/.

- Optional test cases: https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/os/test-cases/kmip-v2.0/optional/.

**Related work:**

This specification replaces or supersedes:

- *Key Management Interoperability Protocol Profiles Version 1.4*. Edited by Tim Hudson and Robert Lockhart. 22 November 2017. OASIS Standard. http://docs.oasis-open.org/kmip/profiles/v1.4/os/kmip-profiles-v1.4-os.html. Latest version: http://docs.oasis-open.org/kmip/profiles/v1.4/kmip-profiles-v1.4.html.

This specification is related to:

- *Key Management Interoperability Protocol Specification Version 2.0*. Edited by Tony Cox and Charles White. Latest version: https://docs.oasis-open.org/kmip/kmip-spec/v2.0/kmip-spec-v2.0.html.

- *Key Management Interoperability Protocol Test Cases Version 2.0. Edited by Tim Hudson* and Mark Joseph. Latest version: https://docs.oasis-open.org/kmip/kmip-testcases/v2.0/kmip-testcases-v2.0.html.

- *Key Management Interoperability Protocol Usage Guide Version 2.0.* Edited by Judith Furlong. Latest version: https://docs.oasis-open.org/kmip/kmip-ug/v2.0/kmip-ug-v2.0.html.

**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 membership of OASIS 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. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip#technical.

TC members should send comments on this specification to the TC’s email list. Others should send comments to the TC’s public comment list, after subscribing to it by following the instructions at the “Send A Comment” button on the TC’s web page at https://www.oasis-open.org/committees/kmip/.

This specification is provided under the RF on RAND Terms Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established. 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 TC’s web page (https://www.oasis-open.org/committees/kmip/ipr.php).

Note that any machine-readable content (Computer Language Definitions) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

**Citation format:**

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

**[kmip-profiles-v2.0]**

*Key Management Interoperability Protocol Profiles Version 2.0*. Edited by Tim Hudson and Robert Lockhart. 31 October 2019. OASIS Standard. https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/os/kmip-profiles-v2.0-os.html. Latest version: https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/kmip-profiles-v2.0.html.

Copyright © OASIS Open 2019. 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.

1 Introduction

1.1 IPR Policy

1.2 Terminology

1.3 Normative References

1.4 Non-Normative References

2 Profiles

2.1 Profile Requirements

2.2 Guidelines for other Profiles

3 Authentication Suites

3.1 Basic Authentication Suite

3.1.1 Basic Authentication Protocols

3.1.2 Basic Authentication Cipher Suites

3.1.3 Basic Authentication Client Authenticity

3.1.4 Basic Authentication KMIP Port Number

3.2 HTTPS Authentication Suite

3.2.1 HTTPS Protocols

3.2.2 HTTPS Cipher Suites

3.2.3 HTTPS Authenticity

3.2.4 HTTPS KMIP Port Number

4 Conformance Test Cases

4.1 Permitted Test Case Variations

4.1.1 Variable Items

4.1.2 Variable behavior

5 Profiles

5.1 Base Profiles

5.1.1 Baseline Client

5.1.2 Baseline Server

5.1.3 Baseline Mandatory Test Cases KMIP v2.0

5.1.3.1 BL-M-1-20

5.1.3.2 BL-M-2-20

5.1.3.3 BL-M-3-20

5.1.3.4 BL-M-4-20

5.1.3.5 BL-M-5-20

5.1.3.6 BL-M-6-20

5.1.3.7 BL-M-7-20

5.1.3.8 BL-M-8-20

5.1.3.9 BL-M-9-20

5.1.3.10 BL-M-10-20

5.1.3.11 BL-M-11-20

5.1.3.12 BL-M-12-20

5.1.3.13 BL-M-13-20

5.2 Complete Server Profile

5.3 HTTPS Profiles

5.3.1 HTTPS Client

5.3.2 HTTPS Server

5.3.3 HTTPS Mandatory Test Cases KMIP v2.0

5.3.3.1 MSGENC-HTTPS-M-1-20

5.4 XML Profiles

5.4.1 XML Encoding

5.4.1.1 Normalizing Names

5.4.1.2 Hex representations

5.4.1.3 Tags

5.4.1.4 Type

5.4.1.5 Value

5.4.1.6 XML Element Encoding

5.4.1.6.1 Tags

5.4.1.6.2 Structure

5.4.1.6.3 Integer

5.4.1.6.4 Integer - Special case for Masks

5.4.1.6.5 Long Integer

5.4.1.6.6 Big Integer

5.4.1.6.7 Enumeration

5.4.1.6.8 Boolean

5.4.1.6.9 Text String

5.4.1.6.10 Byte String

5.4.1.6.11 Date-Time

5.4.1.6.12 Interval

5.4.1.6.13 Date-Time Extended

5.4.2 XML Client

5.4.3 XML Server

5.4.4 XML Mandatory Test Cases KMIP v2.0

5.4.4.1 MSGENC-XML-M-1-20

5.5 JSON Profiles

5.5.1 JSON Encoding

5.5.1.1 Normalizing Names

5.5.1.2 Hex representations

5.5.1.3 Tags

5.5.1.4 Type

5.5.1.5 Value

5.5.1.6 JSON Object

5.5.1.6.1 Tags

5.5.1.6.2 Structure

5.5.1.6.3 Integer

5.5.1.6.4 Integer - Special case for Masks

5.5.1.6.5 Long Integer

5.5.1.6.6 Big Integer

5.5.1.6.7 Enumeration

5.5.1.6.8 Boolean

5.5.1.6.9 Text String

5.5.1.6.10 Byte String

5.5.1.6.11 Date-Time

5.5.1.6.12 Interval

5.5.1.6.13 Date Time Extended

5.5.2 JSON Client

5.5.3 JSON Server

5.5.4 JSON Mandatory Test Cases KMIP v2.0

5.5.4.1 MSGENC-JSON-M-1-20

5.6 Symmetric Key Lifecycle Profiles

5.6.1 Symmetric Key Lifecycle Client

5.6.2 Symmetric Key Lifecycle Server

5.6.3 Symmetric Key Lifecycle Mandatory Test Cases KMIP v2.0

5.6.3.1 SKLC-M-1-20

5.6.3.2 SKLC-M-2-20

5.6.3.3 SKLC-M-3-20

5.6.4 Symmetric Key Lifecycle Optional Test Cases KMIP v2.0

5.6.4.1 SKLC-O-1-20

5.7 Symmetric Key Foundry for FIPS 140 Profiles

5.7.1 Basic Symmetric Key Foundry Client

5.7.2 Intermediate Symmetric Key Foundry Client

5.7.3 Advanced Symmetric Key Foundry Client

5.7.4 Symmetric Key Foundry Server

5.7.5 Basic Symmetric Key Foundry Mandatory Test Cases KMIP v2.0

5.7.5.1 SKFF-M-1-20

5.7.5.2 SKFF-M-2-20

5.7.5.3 SKFF-M-3-20

5.7.5.4 SKFF-M-4-20

5.7.6 Intermediate Symmetric Key Foundry Mandatory Test Cases KMIP v2.0

5.7.6.1 SKFF-M-5-20

5.7.6.2 SKFF-M-6-20

5.7.6.3 SKFF-M-7-20

5.7.6.4 SKFF-M-8-20

5.7.7 Advanced Symmetric Key Foundry Mandatory Test Cases KMIP v2.0

5.7.7.1 SKFF-M-9-20

5.7.7.2 SKFF-M-10-20

5.7.7.3 SKFF-M-11-20

5.7.7.4 SKFF-M-12-20

5.8 Asymmetric Key Lifecycle Profiles

5.8.1 Asymmetric Key Lifecycle Client

5.8.2 Asymmetric Key Lifecycle Server

5.8.3 Asymmetric Key Lifecycle Mandatory Test Cases KMIP v2.0

5.8.3.1 AKLC-M-1-20

5.8.3.2 AKLC-M-2-20

5.8.3.3 AKLC-M-3-20

5.8.4 Asymmetric Key Lifecycle Optional Test Cases KMIP v2.0

5.8.4.1 AKLC-O-1-20

5.9 Cryptographic Profiles

5.9.1 Basic Cryptographic Client

5.9.2 Advanced Cryptographic Client

5.9.3 RNG Cryptographic Client

5.9.4 Basic Cryptographic Server

5.9.5 Advanced Cryptographic Server

5.9.6 RNG Cryptographic Server

5.9.7 Basic Cryptographic Mandatory Test Cases KMIP v2.0

5.9.7.1 CS-BC-M-1-20

5.9.7.2 CS-BC-M-2-20

5.9.7.3 CS-BC-M-3-20

5.9.7.4 CS-BC-M-4-20

5.9.7.5 CS-BC-M-5-20

5.9.7.6 CS-BC-M-6-20

5.9.7.7 CS-BC-M-7-20

5.9.7.8 CS-BC-M-8-20

5.9.7.9 CS-BC-M-9-20

5.9.7.10 CS-BC-M-10-20

5.9.7.11 CS-BC-M-11-20

5.9.7.12 CS-BC-M-12-20

5.9.7.13 CS-BC-M-13-20

5.9.7.14 CS-BC-M-14-20

5.9.7.15 CS-BC-M-GCM-1-20

5.9.7.16 CS-BC-M-GCM-2-20

5.9.7.17 CS-BC-M-GCM-3-20

5.9.7.18 CS-BC-M-CHACHA20-1-20

5.9.7.19 CS-BC-M-CHACHA20-2-20

5.9.7.20 CS-BC-M-CHACHA20-3-20

5.9.7.21 CS-BC-M-CHACHA20POLY1305-1-20

5.9.8 Advanced Cryptographic Mandatory Test Cases KMIP v2.0

5.9.8.1 CS-AC-M-1-20

5.9.8.2 CS-AC-M-2-20

5.9.8.3 CS-AC-M-3-20

5.9.8.4 CS-AC-M-4-20

5.9.8.5 CS-AC-M-5-20

5.9.8.6 CS-AC-M-6-20

5.9.8.7 CS-AC-M-7-20

5.9.8.8 CS-AC-M-8-20

5.9.8.9 CS-AC-M-OAEP-1-20

5.9.8.10 CS-AC-M-OAEP-2-20

5.9.8.11 CS-AC-M-OAEP-3-20

5.9.8.12 CS-AC-M-OAEP-4-20

5.9.8.13 CS-AC-M-OAEP-5-20

5.9.8.14 CS-AC-M-OAEP-6-20

5.9.8.15 CS-AC-M-OAEP-7-20

5.9.8.16 CS-AC-M-OAEP-8-20

5.9.8.17 CS-AC-M-OAEP-9-20

5.9.8.18 CS-AC-M-OAEP-10-20

5.9.9 RNG Cryptographic Mandatory Test Cases KMIP v2.0

5.9.9.1 CS-RNG-M-1-20

5.9.10 RNG Cryptographic Optional Test Cases KMIP v2.0

5.9.10.1 CS-RNG-O-1-20

5.9.10.2 CS-RNG-O-2-20

5.9.10.3 CS-RNG-O-3-20

5.9.10.4 CS-RNG-O-4-20

5.10 Opaque Managed Object Store Profiles

5.10.1 Opaque Managed Object Store Client

5.10.2 Opaque Managed Object Store Server

5.10.3 Opaque Managed Object Mandatory Test Cases KMIP v2.0

5.10.3.1 OMOS-M-1-20

5.10.4 Opaque Managed Object Optional Test Cases KMIP v2.0

5.10.4.1 OMOS-O-1-20

5.11 Storage Array with Self-Encrypting Drives Profiles

5.11.1 Storage Array with Self-Encrypting Drives Client

5.11.2 Storage Array with Self-Encrypting Drives Server

5.11.3 Storage Array with Self-Encrypting Drives Mandatory Test Cases KMIP v2.0

5.11.3.1 SASED-M-1-20

5.11.3.2 SASED-M-2-20

5.11.3.3 SASED-M-3-20

5.12 Tape Library Profiles

5.12.1 Tape Library Profiles Terminology

5.12.2 Tape Library Application Specific Information

5.12.3 Tape Library Alternative Name

5.12.4 Tape Library Client

5.12.5 Tape Library Server

5.12.6 Tape Library Mandatory Test Cases KMIP v2.0

5.12.6.1 TL-M-1-20

5.12.6.2 TL-M-2-20

5.12.6.3 TL-M-3-20

5.13 AES XTS Profiles

5.13.1 AES XTS Client

5.13.2 AES XTS Server

5.13.3 AES XTS Mandatory Test Cases KMIP v2.0

5.13.3.1 AX-M-1-20

5.13.3.2 AX-M-2-20

5.14 Quantum Safe Profiles

5.15 Quantum Safe Client

5.16 Quantum Safe Server

5.17 Mandatory Quantum Safe Test Cases KMIP v2.0

5.17.1 QS-M-1-12 - Query

5.17.2 QS-M-2-20 - Create

5.18 PKCS#11 Profiles

5.18.1 PKCS#11 Encoding

5.18.2 PKCS#11 Examples

5.18.2.1 PKCS#11 Initialization

5.18.2.2 PKCS#11 C_Encrypt

5.18.2.3 PKCS#11 C_GetAttributeValue

5.18.3 PKCS#11 Client

5.18.4 PKCS#11 Server

5.18.5 PKCS#11 Mandatory Test Cases KMIP v2.0

5.18.5.1 PKCS11-M-1-20

6 Conformance

6.1 Baseline Client Basic KMIP v2.0 Profile Conformance

6.2 Baseline Server Basic KMIP v2.0 Profile Conformance

6.3 Complete Server Basic KMIP v2.0 Profile Conformance

6.4 HTTPS Client KMIP v2.0 Profile Conformance

6.5 HTTPS Server KMIP v2.0 Profile Conformance

6.6 XML Client KMIP v2.0 Profile Conformance

6.7 XML Server KMIP v2.0 Profile Conformance

6.8 JSON Client KMIP v2.0 Profile Conformance

6.9 JSON Server KMIP v2.0 Profile Conformance

6.10 Symmetric Key Lifecycle Client KMIP v2.0 Profile Conformance

6.11 Symmetric Key Lifecycle Server KMIP v2.0 Profile Conformance

6.12 Basic Symmetric Key Foundry Client KMIP v2.0 Profile Conformance

6.13 Intermediate Symmetric Key Foundry Client KMIP v2.0 Profile Conformance

6.14 Advanced Symmetric Key Foundry Client KMIP v2.0 Profile Conformance

6.15 Symmetric Key Foundry Server KMIP v2.0 Profile Conformance

6.16 Asymmetric Key Lifecycle Client KMIP v2.0 Profile Conformance

6.17 Asymmetric Key Lifecycle Server KMIP v2.0 Profile Conformance

6.18 Basic Cryptographic Client KMIP v2.0 Profile Conformance

6.19 Advanced Cryptographic Client KMIP v2.0 Profile Conformance

6.20 RNG Cryptographic Client KMIP v2.0 Profile Conformance

6.21 Basic Cryptographic Server KMIP v2.0 Profile Conformance

6.22 Advanced Cryptographic Server KMIP v2.0 Profile Conformance

6.23 RNG Cryptographic Server KMIP v2.0 Profile Conformance

6.24 Opaque Managed Object Client KMIP v2.0 Profile Conformance

6.25 Opaque Managed Object Server KMIP v2.0 Profile Conformance

6.26 Storage Array with Self-Encrypting Drives Client KMIP v2.0 Profile Conformance

6.27 Storage Array with Self-Encrypting Drives Server KMIP v2.0 Profile Conformance

6.28 Tape Library Client KMIP v2.0 Profile Conformance

6.29 Tape Library Server KMIP v2.0 Profile Conformance

6.30 AES XTS Client KMIP v2.0 Profile Conformance

6.31 AES XTS Server KMIP v2.0 Profile Conformance

6.32 Quantum Safe Client KMIP V2.0 Profile Conformance

6.33 Quantum Safe Server KMIP V2.0 Profile Conformance

6.34 PKCS#11 Client KMIP V2.0 Profile Conformance

6.35 PKCS#11 Server KMIP V2.0 Profile Conformance

Appendix A. Acknowledgments

Appendix B. Revision History