Key Management Interoperability Protocol Specification Version 2.0

Key Management Interoperability Protocol Specification Version 2.0

OASIS Standard

31 October 2019

This version:

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

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

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

Previous version:

https://docs.oasis-open.org/kmip/kmip-spec/v2.0/csd01/kmip-spec-v2.0-csd01.docx (Authoritative) https://docs.oasis-open.org/kmip/kmip-spec/v2.0/csd01/kmip-spec-v2.0-csd01.html

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

Latest version:

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

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

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

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

Charles White (chuck@fornetix.com), Fornetix

Related work:

This specification replaces or supersedes:

- *Key Management Interoperability Protocol Specification Version 1.4*. Edited by Tony Cox. OASIS Standard. Latest version: https://docs.oasis-open.org/kmip/spec/v1.4/kmip-spec-v1.4.html.

This specification is related to:

- *Key Management Interoperability Protocol Profiles Version 2.0.* Edited by Tim Hudson and Robert Lockhart. Latest version: https://docs.oasis-open.org/kmip/kmip-profiles/v2.0/kmip-profiles-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-spec-v2.0]

Key Management Interoperability Protocol Specification Version 2.0. Edited by Tony Cox and Charles White. 31 October 2019. OASIS Standard. https://docs.oasis-open.org/kmip/kmip-spec/v2.0/os/kmip-spec-v2.0-os.html. Latest version: https://docs.oasis-open.org/kmip/kmip-spec/v2.0/kmip-spec-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

1.5 Item Data Types

2 Objects

2.1 Certificate

2.2 Certificate Request

2.3 Opaque Object

2.4 PGP Key

2.5 Private Key

2.6 Public Key

2.7 Secret Data

2.8 Split Key

2.9 Symmetric Key

3 Object Data Structures

3.1 Key Block

3.2 Key Value

3.3 Key Wrapping Data

3.4 Transparent Symmetric Key

3.5 Transparent DSA Private Key

3.6 Transparent DSA Public Key

3.7 Transparent RSA Private Key

3.8 Transparent RSA Public Key

3.9 Transparent DH Private Key

3.10 Transparent DH Public Key

3.11 Transparent EC Private Key

3.12 Transparent EC Public Key

4 Object Attributes

4.1 Activation Date

4.2 Alternative Name

4.3 Always Sensitive

4.4 Application Specific Information

4.5 Archive Date

4.6 Certificate Attributes

4.7 Certificate Type

4.8 Certificate Length

4.9 Comment

4.10 Compromise Date

4.11 Compromise Occurrence Date

4.12 Contact Information

4.13 Cryptographic Algorithm

4.14 Cryptographic Domain Parameters

4.15 Cryptographic Length

4.16 Cryptographic Parameters

4.17 Cryptographic Usage Mask

4.18 Deactivation Date

4.19 Description

4.20 Destroy Date

4.21 Digest

4.22 Digital Signature Algorithm

4.23 Extractable

4.24 Fresh

4.25 Initial Date

4.26 Key Format Type

4.27 Key Value Location

4.28 Key Value Present

4.29 Last Change Date

4.30 Lease Time

4.31 Link

4.32 Name

4.33 Never Extractable

4.34 NIST Key Type

4.35 Object Group

4.36 Object Type

4.37 Opaque Data Type

4.38 Original Creation Date

4.39 PKCS#12 Friendly Name

4.40 Process Start Date

4.41 Protect Stop Date

4.42 Protection Level

4.43 Protection Period

4.44 Protection Storage Mask

4.45 Quantum Safe

4.46 Random Number Generator

4.47 Revocation Reason

4.48 Sensitive

4.49 Short Unique Identifier

4.50 State

4.51 Unique Identifier

4.52 Usage Limits

4.53 Vendor Attribute

4.54 X.509 Certificate Identifier

4.55 X.509 Certificate Issuer

4.56 X.509 Certificate Subject

5 Attribute Data Structures

5.1 Attributes

5.2 Common Attributes

5.3 Private Key Attributes

5.4 Public Key Attributes

5.5 Attribute Reference

5.6 Current Attribute

5.7 New Attribute

6 Operations

6.1 Client-to-Server Operations

6.1.1 Activate

6.1.2 Add Attribute

6.1.3 Adjust Attribute

6.1.4 Archive

6.1.5 Cancel

6.1.6 Certify

6.1.7 Check

6.1.8 Create

6.1.9 Create Key Pair

6.1.10 Create Split Key

6.1.11 Decrypt

6.1.12 Delegated Login

6.1.13 Delete Attribute

6.1.14 Derive Key

6.1.15 Destroy

6.1.16 Discover Versions

6.1.17 Encrypt

6.1.18 Export

6.1.19 Get

6.1.20 Get Attributes

6.1.21 Get Attribute List

6.1.22 Get Usage Allocation

6.1.23 Hash

6.1.24 Import

6.1.25 Interop

6.1.26 Join Split Key

6.1.27 Locate

6.1.28 Log

6.1.29 Login

6.1.30 Logout

6.1.31 MAC

6.1.32 MAC Verify

6.1.33 Modify Attribute

6.1.34 Obtain Lease

6.1.35 PKCS#11

6.1.36 Poll

6.1.37 Query

6.1.38 Recover

6.1.39 Register

6.1.40 Revoke

6.1.41 Re-certify

6.1.42 Re-key

6.1.43 Re-key Key Pair

6.1.44 Re-Provision

6.1.45 RNG Retrieve

6.1.46 RNG Seed

6.1.47 Set Attribute

6.1.48 Set Endpoint Role

6.1.49 Sign

6.1.50 Signature Verify

6.1.51 Validate

6.2 Server-to-Client Operations

6.2.1 Discover Versions

6.2.2 Notify

6.2.3 Put

6.2.4 Query

6.2.5 Set Endpoint Role

7 Operations Data Structures

7.1 Authenticated Encryption Additional Data

7.2 Authenticated Encryption Tag

7.3 Capability Information

7.4 Correlation Value

7.5 Data

7.6 Data Length

7.7 Defaults Information

7.8 Derivation Parameters

7.9 Extension Information

7.10 Final Indicator

7.11 Interop Function

7.12 Interop Identifier

7.13 Init Indicator

7.14 Key Wrapping Specification

7.15 Log Message

7.16 MAC Data

7.17 Objects

7.18 Object Defaults

7.19 Operations

7.20 PKCS#11 Function

7.21 PKCS#11 Input Parameters

7.22 PKCS#11 Interface

7.23 PKCS#11 Output Parameters

7.24 PKCS#11 Return Code

7.25 Profile Information

7.26 Profile Version

7.27 Protection Storage Masks

7.28 Right

7.29 Rights

7.30 RNG Parameters

7.31 Server Information

7.32 Signature Data

7.33 Ticket

7.34 Usage Limits

7.35 Validation Information

8 Messages

8.1 Request Message

8.2 Request Header

8.3 Request Batch Item

8.4 Response Message

8.5 Response Header

8.6 Response Batch Item

9 Message Data Structures

9.1 Asynchronous Correlation Value

9.2 Asynchronous Indicator

9.3 Attestation Capable Indicator

9.4 Authentication

9.5 Batch Count

9.6 Batch Error Continuation Option

9.7 Batch Item

9.8 Batch Order Option

9.9 Correlation Value (Client)

9.10 Correlation Value (Server)

9.11 Credential

9.12 Maximum Response Size

9.13 Message Extension

9.14 Nonce

9.15 Operation

9.16 Protocol Version

9.17 Result Message

9.18 Result Reason

9.19 Result Status

9.20 Time Stamp

9.21 Unique Batch Item ID

10 Message Protocols

10.1 TTLV

10.1.1 Tag

10.1.2 Type

10.1.3 Length

10.1.4 Value

10.1.5 Padding

10.2 Other Message Protocols

10.2.1 HTTPS

10.2.2 JSON

10.2.3 XML

10.3 Authentication

10.4 Transport

11 Enumerations

11.1 Adjustment Type Enumeration

11.2 Alternative Name Type Enumeration

11.3 Asynchronous Indicator Enumeration

11.4 Attestation Type Enumeration

11.5 Batch Error Continuation Option Enumeration

11.6 Block Cipher Mode Enumeration

11.7 Cancellation Result Enumeration

11.8 Certificate Request Type Enumeration

11.9 Certificate Type Enumeration

11.10 Client Registration Method Enumeration

11.11 Credential Type Enumeration

11.12 Cryptographic Algorithm Enumeration

11.13 Data Enumeration

11.14 Derivation Method Enumeration

11.15 Destroy Action Enumeration

11.16 Digital Signature Algorithm Enumeration

11.17 DRBG Algorithm Enumeration

11.18 Encoding Option Enumeration

11.19 Endpoint Role Enumeration

11.20 FIPS186 Variation Enumeration

11.21 Hashing Algorithm Enumeration

11.22 Interop Function Enumeration

11.23 Item Type Enumeration

11.24 Key Compression Type Enumeration

11.25 Key Format Type Enumeration

11.26 Key Role Type Enumeration

11.27 Key Value Location Type Enumeration

11.28 Link Type Enumeration

11.29 Key Wrap Type Enumeration

11.30 Mask Generator Enumeration

11.31 Name Type Enumeration

11.32 NIST Key Type Enumeration

11.33 Object Group Member Enumeration

11.34 Object Type Enumeration

11.35 Opaque Data Type Enumeration

11.36 Operation Enumeration

11.37 Padding Method Enumeration

11.38 PKCS#11 Function Enumeration

11.39 PKCS#11 Return Code Enumeration

11.40 Profile Name Enumeration

11.41 Protection Level Enumeration

11.42 Put Function Enumeration

11.43 Query Function Enumeration

11.44 Recommended Curve Enumeration

11.45 Result Reason Enumeration

11.46 Result Status Enumeration

11.47 Revocation Reason Code Enumeration

11.48 RNG Algorithm Enumeration

11.49 RNG Mode Enumeration

11.50 Secret Data Type Enumeration

11.51 Shredding Algorithm Enumeration

11.52 Split Key Method Enumeration

11.53 State Enumeration

11.54 Tag Enumeration

11.55 Ticket Type Enumeration

11.56 Unique Identifier Enumeration

11.57 Unwrap Mode Enumeration

11.58 Usage Limits Unit Enumeration

11.59 Validity Indicator Enumeration

11.60 Wrapping Method Enumeration

11.61 Validation Authority Type Enumeration

11.62 Validation Type Enumeration

12 Bit Masks

12.1 Cryptographic Usage Mask

12.2 Protection Storage Mask

12.3 Storage Status Mask

13 Algorithm Implementation

13.1 Split Key Algorithms

14 KMIP Client and Server Implementation Conformance

14.1 KMIP Client Implementation Conformance

14.2 KMIP Server Implementation Conformance

Appendix A. Acknowledgments

Appendix B. Acronyms

Appendix C. List of Figures and Tables

Appendix D. Revision History