



Key Management Interoperability Protocol Specification Version 1.4 Errata 01

Committee Specification Draft 01 / Public Review Draft 01

30 May 2019

This version:

<https://docs.oasis-open.org/kmip/spec/v1.4/errata01/csprd01/kmip-spec-v1.4-errata01-csprd01.docx>
(Authoritative)
<https://docs.oasis-open.org/kmip/spec/v1.4/errata01/csprd01/kmip-spec-v1.4-errata01-csprd01.html>
<https://docs.oasis-open.org/kmip/spec/v1.4/errata01/csprd01/kmip-spec-v1.4-errata01-csprd01.pdf>

Previous version:

N/A

Latest version:

<https://docs.oasis-open.org/kmip/spec/v1.4/errata01/kmip-spec-v1.4-errata01.docx> (Authoritative)
<https://docs.oasis-open.org/kmip/spec/v1.4/errata01/kmip-spec-v1.4-errata01.html>
<https://docs.oasis-open.org/kmip/spec/v1.4/errata01/kmip-spec-v1.4-errata01.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

Editor:

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

Additional artifacts:

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

- *Key Management Interoperability Protocol Specification Version 1.4 Plus Errata 01*. Edited by Tony Cox. 30 May 2019. OASIS Standard incorporating Public Review Draft 01 of Errata 01.
<https://docs.oasis-open.org/kmip/spec/v1.4/errata01/csprd01/kmip-spec-v1.4-errata01-csprd01-redlined.html>.

Related work:

This specification replaces or supersedes:

- *Key Management Interoperability Protocol Specification Version 1.0*. Edited by Robert Haas and Indra Fitzgerald. 01 October 2010. OASIS Standard. <http://docs.oasis-open.org/kmip/spec/v1.0/os/kmip-spec-1.0-os.html>.
- *Key Management Interoperability Protocol Specification Version 1.1*. Edited by Robert Haas and Indra Fitzgerald. 24 January 2013. OASIS Standard. <http://docs.oasis-open.org/kmip/spec/v1.1/os/kmip-spec-v1.1-os.html>.

- *Key Management Interoperability Protocol Specification Version 1.2*. Edited by Kiran Thota and Kelley Burgin. 19 May 2015. OASIS Standard. <http://docs.oasis-open.org/kmip/spec/v1.2/os/kmip-spec-v1.2-os.html>.
- *Key Management Interoperability Protocol Specification Version 1.3*. Edited by Kiran Thota and Tony Cox. 27 December 2016. OASIS Standard. <http://docs.oasis-open.org/kmip/spec/v1.3/os/kmip-spec-v1.3-os.html>.

Abstract:

This document lists errata for the *Key Management Interoperability Protocol Specification Version 1.4 OASIS Standard*. It 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 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. 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-v1.4-errata01]

Key Management Interoperability Protocol Specification Version 1.4 Errata 01. Edited by Tony Cox. 30 May 2019. Committee Specification Draft 01 / Public Review Draft 01. <https://docs.oasis-open.org/kmip/spec/v1.4/errata01/csprd01/kmip-spec-v1.4-errata01-csprd01.html>. Latest version: <https://docs.oasis-open.org/kmip/spec/v1.4/errata01/kmip-spec-v1.4-errata01.html>.

Notices

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.

Table of Contents

1	Introduction	5
1.1	IPR Policy	5
1.2	Terminology	5
1.3	Normative References	5
2	List of Errata	6
2.1	§2.2, page 37	6
2.2	§2.2.8, page 40	6
2.3	Table 104: State Attribute Rules, page 65.....	6
3	Conformance	7
	Appendix A. Acknowledgments	8
	Appendix B. Revision History	10

1 Introduction

This document lists the approved errata to the OASIS KMIP v1.4 OASIS Standard. Each one has a number that refers to the issue that triggered the erratum.

As required by the OASIS Technical Committee Process, the approved errata represent changes that are not “substantive”. The changes focus on clarifications to ambiguous or conflicting specification text, where different compliant implementations might have reasonably chosen different interpretations. The intent of the KMIP TC has been to resolve such issues in service of improved interoperability based on subsequent normative works as well as implementation and deployment experience.

In this document, errata change instructions are presented with surrounding context as necessary to make the intent clear. Original specification text is often presented as follows, with problem text highlighted in bold:

This is an original specification sentence. **The second sentence needs to be changed, removed, or replaced.**

New specification text is typically presented as follows, with new or changed text highlighted in bold:

This is a highly original specification sentence. **This is the wholly new content to replace the old second sentence. It runs on and on and on.**

In a few cases, text needs only to be struck, in which case the change is shown as follows, with text to be removed both highlighted in bold and struck through:

This is yet another original specification sentence which contains ~~**an inappropriately**~~ long description.

In addition to this normative document, non-normative “errata composite” documents may be provided that combine the prescribed corrections with the original specification text, illustrating the changes with margin change bars, struck-through original text, and highlighted new text. These documents, if available, will be found at the same location as this approved form..

1.1 IPR Policy

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>).

1.2 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]] and [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.3 Normative References

- | | |
|------------------|--|
| [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 >. |
| [RFC8174] | Leiba, B., “Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words”, BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, < http://www.rfc-editor.org/info/rfc8174 >. |

2 List of Errata

The Errata items contained within this document are all focused on clarifying lifecycle and operational usage of Opaque Objects. As such the following

2.1 §2.2, page 37

Remove the text

Managed Objects are objects that are the subjects of key management operations, which are described in Sections 4 and 5. Managed Cryptographic Objects are the subset of Managed Objects that contain cryptographic material ~~(e.g., certificates, keys, and secret data)~~.

2.2 §2.2.8, page 40

Add the text

A Managed Object that the key management server is possibly not able to interpret. The context information for this object MAY be stored and retrieved using Custom Attributes.

An Opaque Object MAY be a Managed Cryptographic Object depending on the client context of usage and as such is treated in the same manner as a Managed Cryptographic Object for handling of attributes.

2.3 Table 104: State Attribute Rules, page 65

Remove the text

All ~~Cryptographic~~ Objects

3 Conformance

These changes will not require any changes to the conformance rules for KMIP Specification v1.4. The Conformance section of the KMIP Specification v1.4 OASIS Standard is unchanged.

Appendix A. Acknowledgments

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

Participants:

Rinkesh Bansal - IBM
Jeff Bartell - Individual
Gabriel Becker - KRYPTUS
Andre Bereza - KRYPTUS
Anthony Berglas - Cryptsoft Pty Ltd.
Mathias Bjorkqvist - IBM
Joseph Brand - Semper Fortis Solutions
Alan Brown - Thales e-Security
Andrew Byrne - Dell
Tim Chevalier - NetApp
Kenli Chong - QuintessenceLabs Pty Ltd.
Justin Corlett - Cryptsoft Pty Ltd.
Tony Cox - Cryptsoft Pty Ltd.
James Crossland - Northrop Grumman
Stephen Edwards - Semper Fortis Solutions
Stan Feather - Hewlett Packard Enterprise (HPE)
Indra Fitzgerald - Utimaco IS GmbH
Judith Furlong - Dell
Gary Gardner - Fornetix
Susan Gleeson - Oracle
Steve He - Thales e-Security
Christopher Hillier - Hewlett Packard Enterprise (HPE)
Tim Hudson - Cryptsoft Pty Ltd.
Nitin Jain - SafeNet, Inc.
Gershon Janssen - Individual
Mark Joseph - P6R, Inc
Paul Lechner - KeyNexus Inc
John Leiseboer - QuintessenceLabs Pty Ltd.
Jarrett Lu - Oracle
Jeff MacMillan - KeyNexus Inc
John Major - QuintessenceLabs Pty Ltd.
Cecilia Majorel - Quintessence Labs
Gabriel Mandaji - KRYPTUS
Jon Mentzell - Fornetix
Prashant Mestri - IBM
Kevin Mooney - Fornetix
Ladan Nekuii - Thales e-Security

Jason Novecosky - KeyNexus Inc
Matt O'reilly - Fernetix
Sanjay Panchal - IBM
Mahesh Paradkar - IBM
Steve Pate - Thales e-Security
Greg Pepus - Semper Fortis Solutions
Bruce Rich - Cryptsoft Pty Ltd.
Thad Roemer - Dyadic Security Ltd.
Thad Roemer - Unbound Tech
Greg Scott - Cryptsoft Pty Ltd.
Martin Shannon - QuintessenceLabs Pty Ltd.
Gerald Stueve - Fernetix
Jim Susoy - P6R, Inc
Jason Thatcher - Cryptsoft Pty Ltd.
Peter Tsai - Thales e-Security
Charles White - Fernetix
Steven Wierenga - Utimaco IS GmbH
Kyle Wuolle - KeyNexus Inc

Appendix B. Revision History

Revision	Date	Editor	Changes Made
WD01	2 May 2019	Tony Cox	Clarification of Opaque object handling
WD02	23 May 2019	Tony Cox	Added related documents section and updated required (non-material) text.