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


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/).

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]
# 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

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 - Fornetix
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 - Fornetix
Jim Susoy - P6R, Inc
Jason Thatcher - Cryptsoft Pty Ltd.
Peter Tsai - Thales e-Security
Charles White - Fornetix
Steven Wierenga - Utimaco IS GmbH
Kyle Wuolle - KeyNexus Inc
## Appendix B. Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Editor</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>WD01</td>
<td>2 May 2019</td>
<td>Tony Cox</td>
<td>Clarification of Opaque object handling</td>
</tr>
<tr>
<td>WD02</td>
<td>23 May 2019</td>
<td>Tony Cox</td>
<td>Added related documents section and updated required (non-material) text.</td>
</tr>
</tbody>
</table>