PKCS #11 Cryptographic Token Interface Base Specification Version 2.40 Errata 01

OASIS Approved Errata

13 May 2016

Specification URIs

This version:

http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/errata01/os/pkcs11-base-v2.40-errata01-os.doc (Authoritative)
http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/errata01/os/pkcs11-base-v2.40-errata01-os.html
http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/errata01/os/pkcs11-base-v2.40-errata01-os.pdf

Previous version:

N/A

Latest version:

http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/pkcs11-base-v2.40.doc (Authoritative)
http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/pkcs11-base-v2.40.html
http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/pkcs11-base-v2.40.pdf

Technical Committee:

OASIS PKCS 11 TC

Chairs:

Robert Relyea (rrelyea@redhat.com), Red Hat
Valerie Fenwick (valerie.fenwick@oracle.com), Oracle

Editors:

Robert Griffin (robert.griffin@emc.com), EMC Corporation
Tim Hudson (tjh@cryptsoft.com), Cryptsoft Pty Ltd

Additional artifacts:

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

- *PKCS #11 Cryptographic Token Interface Base Specification Version 2.40 Plus Errata 01*. Edited by Susan Gleeson, Chris Zimman, Robert Griffin, and Tim Hudson. 13 May 2016. OASIS Standard Incorporating Approved Errata 01. http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/errata01/os/pkcs11-base-v2.40-errata01-os-complete.html.
- Normative computer language definition files for PKCS #11 v2.40:
  - http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/errata01/os/include/pkcs11-v2.40/pkcs11.h
  - http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/errata01/os/include/pkcs11-v2.40/pkcs11t.h
  - http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/errata01/os/include/pkcs11-v2.40/pkcs11f.h

Related work:

This specification is related to:

- *PKCS #11 Cryptographic Token Interface Base Specification Version 2.40.* Edited by Susan Gleeson and Chris Zimman. 14 April 2015. OASIS Standard. http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.html.

Abstract:

This document contains corrections to errors and omissions in the *PKCS #11 Cryptographic Token Interface Base Specification version 2.40 OASIS Standard*.

Status:

This document was last revised or approved by the OASIS PKCS 11 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=pkcs11#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/pkcs11/.

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/pkcs11/ipr.php).

Citation format:

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

[PKCS11-base-v2.40-Errata01]

PKCS #11 Cryptographic Token Interface Base Specification Version 2.40 Errata 01. Edited by Robert Griffin and Tim Hudson. 13 May 2016. OASIS Approved Errata. http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/errata01/os/pkcs11-base-v2.40-errata01-os.html. Latest version: http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/pkcs11-base-v2.40.html.

Notices

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

[All text is normative unless otherwise labeled]

1.1 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]**.

1.2 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.

[PKCS #11-Base] *PKCS #11 Cryptographic Token Interface Base Specification Version 2.40*. Edited by Susan Gleeson and Chris Zimman. 14 April 2015. OASIS Standard. http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.html. Latest version: http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/pkcs11-base-v2.40.html.

[PKCS #11-Base-Rev01] *PKCS #11 Cryptographic Token Interface Base Specification Version 2.40 Plus Errata 01*. Edited by Susan Gleeson, Chris Zimman, Robert Griffin, and Tim Hudson. 09 December 2015. OASIS Standard Incorporating Draft 01 of Errata 01. http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/errata01/csd01/pkcs11-base-v2.40-errata01-csd01-complete.html.

2 Errata for PKCS #11 Base Specification v2.40 OS

2.1 Removal of Manifest Constants from Appendix B

To minimize the risk of errors, values for PKCS #11 manifest constants in **[PKCS #11-Base-Rev01]** are specified only in the normative computer language definition files associated with that specification. The table of manifest constant definitions that was included in Appendix B of the **[PKCS #11-Base]** is not included in **[PKCS #11-Base-Rev01].** Corrections to errors in Appendix B of **[PKCS #11-Base]** have been incorporated into the normative computer language definition files specified in **[PKCS #11-Base-Rev01].**

See the following normative computer language definition files for the manifest constants:

- include/pkcs11-v2.40/pkcs11.h
- include/pkcs11-v2.40/pkcs11t.h
- include/pkcs11-v2.40/pkcs11f.h

2.2 Corrections to Manifest Constant Definitions

The following definitions were incorrectly specified in **[PKCS #11-Base]:**

- CK_HW_FEATURE_TYPE is correctly specified in section 3.4 of **[PKCS #11-Base]**, but is incorrectly specified as CK_HW_FEATURE in sections 4.3.3.1, 4.3.4.1 and 4.3.5.1 of **[PKCS #11-Base]**, where it should have been referred to as CK_HW_FEATURE_TYPE**.** This error is corrected in **[PKCS #11-Base-Rev01].** In addition, the incorrect CK_HW_FEATURE constant is not included in the PKCS#11 normative computer language definition files.
- CKR_COPY_PROHIBITED was incorrectly specified in Appendix B of **[PKCS #11-Base];** it should not exist and where used is meant to be CKR_ACTION_PROHIBITED, This value should not exist and is not included in the PKCS#11 normative computer language definition files**.**

2.3 Corrections to Functions Macro

The macro CK_DEFINE_FUNCTION was replaced with CK_DECLARE_FUNCTION as this is what is contained in the normative computer language files. CK_DEFINE_FUNCTION was unused and has been removed from the specification and the normative computer language files.

3 PKCS #11 Implementation Conformance

PKCS #11 Implementation Conformance is defined in Section 6 of **[PKCS #11-Base-Rev01].**

Appendix A. Acknowledgments

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

Participants:

Warren Armstrong, QuintessenceLabs Pty Ltd.

Jeff Bartell, Semper Fortis Solutions LLC

Anthony Berglas, Cryptsoft Pty Ltd.

Christian Bollich, Utimaco IS GmbH

Dieter Bong, Utimaco IS GmbH

Robert Burns, Thales e-Security

Andrew Byrne, EMC

Wan-Teh Chang, Google Inc.

Hai-May Chao, Oracle

Janice Cheng, Vormetric, Inc.

Doron Cohen, SafeNet, Inc.

Justin Corlett, Cryptsoft Pty Ltd.

Tony Cox, Cryptsoft Pty Ltd.

Chris Dunn, SafeNet, Inc.

Valerie Fenwick, Oracle

Terry Fletcher, SafeNet, Inc.

Ricardo Foccardi, Cryptosense

Susan Gleeson, Oracle

John Green, QuintessenceLabs Pty Ltd.

Robert Griffin, EMC

Peter Gutmann, Individual

Thomas Hardjono, M.I.T.

Tim Hudson, Cryptsoft Pty Ltd.

Gershon Janssen, Individual

Wang Jingmin, Feitan Technologies Co. Ltd.

Mark Joseph, P6R Inc.

Dina Kurktchi-Nimeh, Oracle

John Leiseboer, QuintessenceLabs Pty Ltd.

Shan Leon, Feitian Technologies Co. Ltd.

Geoffrey Li, Feitian Technologies Co. Ltd.

Howie Liu, Feitian Technologies Co. Ltd.

Hal Lockhart, Oracle

Robert Lockhart, Thales e-Security

Darren Moffat, Oracle

Valery Osheter, SafeNet, Inc.

Sean Parkinson, EMC
Rob Philpott, EMC
Mark Powers, Oracle
Ajai Puri, SafeNet Inc.
Robert Relyea, Red Hat
Greg Scott, Cryptsoft Pty Ltd.
Ryan Smith, Futurex
Graham Steel, Cryptosense
Jim Susoy, P6R Inc.
Sander Temme, Thales e-Security
Kiran Thota, VMware Inc.
Stef Walter, Red Hat
James Wang, Vormetric
Jeff Webb, Dell
Steve Wierenga, Hewlett Packard Enterprise (HPE)
Thomas Xuelin, Watchdata Technologies Ptd Ltd.
Peng Yu, Feitian Technologies Co. Ltd.
Jenny Yung, Oracle
Magda Zdunkiewicz, Cryptsoft Pty Ltd.
Chris Zimman, Individual

Appendix B. Revision History

Revision	Date	Editor	Changes Made
wd01	Dec 9 2015	Robert Griffin / Tim Hudson	First draft, incorporating v2.40 errata from the PKCS 11 TC wiki into template document