



# PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40 Errata 01

Committee Specification Draft 01 /  
Public Review Draft 01

09 December 2015

## Specification URIs

This version:

<http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/errata01/csprd01/pkcs11-curr-v2.40-errata01-csprd01.doc> (Authoritative)

<http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/errata01/csprd01/pkcs11-curr-v2.40-errata01-csprd01.html>

<http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/errata01/csprd01/pkcs11-curr-v2.40-errata01-csprd01.pdf>

Previous version:

N/A

Latest version:

<http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/errata01/pkcs11-curr-v2.40-errata01.doc>  
(Authoritative)

<http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/errata01/pkcs11-curr-v2.40-errata01.html>

<http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/errata01/pkcs11-curr-v2.40-errata01.pdf>

Technical Committee:

OASIS PKCS 11 TC

Chairs:

Robert Relyea ([rrelyea@redhat.com](mailto:rrelyea@redhat.com)), Red Hat

Valerie Fenwick ([valerie.fenwick@oracle.com](mailto:valerie.fenwick@oracle.com)), Oracle

Editors:

Robert Griffin ([robert.griffin@emc.com](mailto:robert.griffin@emc.com)), EMC Corporation

Tim Hudson ([tjh@cryptsoft.com](mailto: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 Current Mechanisms Specification Version 2.40 Plus Errata 01*. Edited by Susan Gleeson, Chris Zimman, Robert Griffin, and Tim Hudson. 09 December 2015. OASIS Standard Incorporating Public Review Draft 01 of Errata 01.

<http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/errata01/csprd01/pkcs11-curr-v2.40-errata01-csprd01-complete.html>.

Related work:

This specification is related to:

- Normative computer language definition files for PKCS #11 v2.40:

- <http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/errata01/csprd01/include/pkcs11-v2.40/pkcs11.h>
- <http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/errata01/csprd01/include/pkcs11-v2.40/pkcs11t.h>
- <http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/errata01/csprd01/include/pkcs11-v2.40/pkcs11f.h>

**Abstract:**

This document contains corrections to errors and omissions in the *PKCS #11 Cryptographic Token Interface Current Mechanisms 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](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-curr-v2.40-Errata01]**

*PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40 Errata 01*. Edited by Robert Griffin and Tim Hudson. 09 December 2015. OASIS Committee Specification Draft 01 / Public Review Draft 01. <http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/errata01/csprd01/pkcs11-curr-v2.40-errata01-csprd01.html>. Latest version: <http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/errata01/pkcs11-curr-v2.40-errata01.html>.

---

## Notices

Copyright © OASIS Open 2015. 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	Terminology .....	5
1.2	Normative References .....	5
2	Errata for PKCS #11 Current Mechanisms Specification v2.40 OS.....	6
2.1	Removal of Manifest Constants from Appendix B .....	6
2.2	Corrections to TLS V1.2 Mechanisms .....	6
2.3	Corrections to PKCS #11 Current Mechanisms Specification V2.40 OS .....	6
3	Conformance .....	9
	Appendix A. Acknowledgments .....	10
	Appendix B. Revision History .....	13

---

# 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]** 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>.

[.

## 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-Curr]** *PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40*. Edited by Susan Gleeson and Chris Zimman. 14 April 2015. OASIS Standard. <http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/os/pkcs11-curr-v2.40-os.html>. Latest version: <http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/pkcs11-curr-v2.40.html>.
- [PKCS #11-Curr-Rev01]** *PKCS #11 Cryptographic Token Interface Current Mechanisms 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-curr/v2.40/errata01/csd01/pkcs11-curr-v2.40-errata01-csd01-complete.html>.

---

## 2 Errata for PKCS #11 Current Mechanisms 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-Curr-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-Curr] is not included in [PKCS #11-Curr-Rev01]. Corrections to errors in Appendix B of [PKCS #11-Curr] have been incorporated into the normative computer language definition files specified in [PKCS #11-Curr-Rev01].

See the following normative computer language definition files (linked from the “[Related work](#)” section above) 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 TLS V1.2 Mechanisms

Implementers of the TLS V1.2 mechanisms as specified in [PKCS #11-Curr] should consult the PKCS 11 TC wiki at <https://wiki.oasis-open.org/pkcs11/> for the latest informative guidance prior to implementing these mechanisms. Refinements to the specification of the TLS V1.2 mechanisms are anticipated as part of PKCS #11 V2.41.

### 2.3 Corrections to PKCS #11 Current Mechanisms Specification V2.40 OS

The following corrections have been made in [PKCS #11-Curr-Rev01]:

- The definition of CK\_SEED\_CBC\_ENCRYPT\_DATA\_PARAMS was omitted from the specification text.

```
typedef struct CK_SEED_CBC_ENCRYPT_DATA_PARAMS {
    CK_BYTE      iv[16];
    CK_BYTE_PTR  pData;
    CK_ULONG     length;
} CK_SEED_CBC_ENCRYPT_DATA_PARAMS;

typedef CK_SEED_CBC_ENCRYPT_DATA_PARAMS CK_PTR
CK_SEED_CBC_ENCRYPT_DATA_PARAMS_PTR;
```

- References to CK\_PARAM\_TYPE have been corrected to CK\_OTP\_PARAM\_TYPE.
- The corrected definition of CK\_PKCS5\_PBKDF2\_PARAMS2 that replaces the deprecated CK\_PKCS5\_PBKD2\_PARAMS was omitted from the specification text.

```
typedef struct CK_PKCS5_PBKD2_PARAMS2 {
    CK_PKCS5_PBKDF2_SALT_SOURCE_TYPE saltSource;
    CK_VOID_PTR  pSaltSourceData;
```

```

    CK_ULONG ulSaltSourceDataLen;
    CK_ULONG iterations;
    CK_PKCS5_PBKD2_PSEUDO_RANDOM_FUNCTION_TYPE prf;
    CK_VOID_PTR pPrfData;
    CK_ULONG ulPrfDataLen;
    CK_UTF8CHAR_PTR pPassword;
    CK_ULONG ulPasswordLen;
} CK_PKCS5_PBKD2_PARAMS2;

```

- References to CKM\_X9\_42\_DH\_PKCS\_PARAMETER\_GEN have been corrected to CKM\_X9\_42\_DH\_PARAMETER\_GEN
- Typographical error of CKM\_AES\_XCBC\_MAC-96 has been corrected to CKM\_AES\_XCBC\_MAC\_96
- In section 2.41.5.1 the CKA\_OTP\_CHALLENGE\_REQUIREMENT table entry had an incorrect line break.
- References to CKA\_OTP\_CHALLENGE\_REQUIREMENT have been corrected to CKA\_OTP\_CHALLENGE\_REQUIREMENT
- References to CK\_CBC\_ENCRYPT\_DATA\_PARAMS have been corrected to CK\_SEED\_CBC\_ENCRYPT\_DATA\_PARAMS
- References to CK\_CBC\_ENCRYPT\_DATA\_PARAMS\_PTR have been corrected to CK\_SEED\_CBC\_ENCRYPT\_DATA\_PARAMS\_PTR
- Missing text in section 2.2.1 CK\_DSA\_PARAMETER\_GEN\_PARAM has been included
  - CK\_DSA\_PARAMETER\_GEN\_PARAM\_PTR is a pointer to a CK\_DSA\_PARAMETER\_GEN\_PARAM
- Typographical error with an extra space in "CK\_ECMQV\_DERIVE\_PARAMS"
- Missing text in section 2.45.5 CK\_GOSTR3410\_DERIVE\_PARAMS has been included
  - CK\_GOSTR3410\_DERIVE\_PARAMS\_PTR is a pointer to a CK\_GOSTR3410\_DERIVE\_PARAMS
- Missing text in section 2.45.5 CK\_GOSTR3410\_KEY\_WRAP\_PARAMS has been included
  - CK\_GOSTR3410\_KEY\_WRAP\_PARAMS\_PTR is a pointer to a CK\_GOSTR3410\_KEY\_WRAP\_PARAMS
- References to CKM\_DSA\_PROBABALISTIC\_PARAMETER\_GEN have been corrected to CKM\_DSA\_PROBABLISTIC\_PARAMETER\_GEN
- References to CKM\_GOSTR3410\_WITH\_GOST3411 have been corrected to CKM\_GOSTR3410\_WITH\_GOSTR3411
- References to CKM\_SHA1 have been corrected to CKM\_SHA\_1
- References to CK\_OTP\_FORMAT have been corrected to CK\_OTP\_OUTPUT\_FORMAT
- References to CK\_PKCS5\_PBKD2\_PARAM have been corrected to CK\_PKCS5\_PBKD2\_PARAMS





---

## 3 Conformance

PKCS #11 Implementation Conformance is defined in Section 3 of **[PKCS #11-Curr]**.

---

## Appendix A. Acknowledgments

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

### Participants:

Gil Abel, Athena Smartcard Solutions, Inc.  
Warren Armstrong, QuintessenceLabs  
Jeff Bartell, Semper Fortis Solutions LLC  
Peter Bartok, Venafi, Inc.  
Anthony Berglas, Cryptsoft  
Joseph Brand, Semper Fortis Solutions LLC  
Kelley Burgin, National Security Agency  
Robert Burns, Thales e-Security  
Wan-Teh Chang, Google Inc.  
Hai-May Chao, Oracle  
Janice Cheng, Vormetric, Inc.  
Sangrae Cho, Electronics and Telecommunications Research Institute (ETRI)  
Doron Cohen, SafeNet, Inc.  
Fadi Cotran, Futurex  
Tony Cox, Cryptsoft  
Christopher Duane, EMC  
Chris Dunn, SafeNet, Inc.  
Valerie Fenwick, Oracle  
Terry Fletcher, SafeNet, Inc.  
Susan Gleeson, Oracle  
Sven Gossel, Charismathics  
John Green, QuintessenceLabs  
Robert Griffin, EMC  
Paul Grojean, Individual  
Peter Gutmann, Individual  
Dennis E. Hamilton, Individual  
Thomas Hardjono, M.I.T.  
Tim Hudson, Cryptsoft  
Gershon Janssen, Individual  
Seunghun Jin, Electronics and Telecommunications Research Institute (ETRI)  
Wang Jingman, Feitan Technologies  
Andrey Jivsov, Symantec Corp.  
Mark Joseph, P6R  
Stefan Kaesar, Infineon Technologies  
Greg Kazmierczak, Wave Systems Corp.

Mark Knight, Thales e-Security  
Darren Krahn, Google Inc.  
Alex Krasnov, Infineon Technologies AG  
Dina Kurktchi-Nimeh, Oracle  
Mark Lambiase, SecureAuth Corporation  
Lawrence Lee, GoTrust Technology Inc.  
John Leiseboer, QuintessenceLabs  
Sean Leon, Infineon Technologies  
Geoffrey Li, Infineon Technologies  
Howie Liu, Infineon Technologies  
Hal Lockhart, Oracle  
Robert Lockhart, Thales e-Security  
Dale Moberg, Axway Software  
Darren Moffat, Oracle  
Valery Osheter, SafeNet, Inc.  
Sean Parkinson, EMC  
Rob Philpott, EMC  
Mark Powers, Oracle  
Ajai Puri, SafeNet, Inc.  
Robert Relyea, Red Hat  
Saikat Saha, Oracle  
Subhash Sankuratipati, NetApp  
Anthony Scarpino, Oracle  
Johann Schoetz, Infineon Technologies AG  
Rayees Shamsuddin, Wave Systems Corp.  
Radhika Siravara, Oracle  
Brian Smith, Mozilla Corporation  
David Smith, Venafi, Inc.  
Ryan Smith, Futurex  
Jerry Smith, US Department of Defense (DoD)  
Oscar So, Oracle  
Graham Steel, Cryptosense  
Michael Stevens, QuintessenceLabs  
Michael StJohns, Individual  
Jim Susoy, P6R  
Sander Temme, Thales e-Security  
Kiran Thota, VMware, Inc.  
Walter-John Turnes, Gemini Security Solutions, Inc.  
Stef Walter, Red Hat  
James Wang, Vormetric  
Jeff Webb, Dell  
Peng Yu, Feitian Technologies

Magda Zdunkiewicz, Cryptsoft  
Chris Zimman, Individual

---

## Appendix B. Revision History

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