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

Committee Specification Draft 01

09 December 2015

Specification URLs
This version:

http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/errata01/csd01/pkcs11-curr-v2.40-errata01-csd01.doc (Authoritative)
http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/errata01/csd01/pkcs11-curr-v2.40-errata01-csd01.html
http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/errata01/csd01/pkcs11-curr-v2.40-errata01-csd01.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), 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:


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/csd01/include/pkcs11-v2.40/pkcs11.h
Abstract:

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-curr-v2.40-Errata01]
# 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


1.2 Normative References


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.

```c
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_PTR 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_PBKDF2_Params was omitted from the specification text.

```c
typedef struct CK_PKCS5_PBKDF2_PARAMS2 {
    CK_PKCS5_PBKDF2_SALT_SOURCE_TYPE saltSource;
    CK_VOID_PTR pSaltSourceData;
```
References to CKM_X9_42_DH_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
  o 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
  o 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
  o CK_GOSTR3410_KEY_WRAP_PARAMS_PTR is a pointer to a CK_GOSTR3410_KEY_WRAP_PARAMS

References to CKM_DSA_PROBABLISTIC_PARAMETER_GEN have been corrected to CKM_DSA_PROBABLISTIC_PARAMETER_GEN

References to CKM_GOSTR3410_WITH_GOST3411 have been corrected to CKM_GOSTR3410_WITH_GOST3411

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.
Magda Zdunkiewicz, Cryptsoft
Chris Zimman, Individual
# 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>9 Dec 2015</td>
<td>Robert Griffin / Tim Hudson</td>
<td>First draft, incorporating v2.40 errata from the PKCS 11 TC wiki into template document</td>
</tr>
</tbody>
</table>