PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 3.0 Errata 01

OASIS Standard with Approved Errata

14 August 2024

This stage:
https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/errata01/cs01/pkcs11-curr-v3.0-errata01-cs01.docx (Authoritative)
https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/errata01/cs01/pkcs11-curr-v3.0-errata01-cs01.html
https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/errata01/cs01/pkcs11-curr-v3.0-errata01-cs01.pdf

Previous stage:
https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/errata01/csd01/pkcs11-curr-v3.0-errata01-csd01.docx (Authoritative)
https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/errata01/csd01/pkcs11-curr-v3.0-errata01-csd01.html
https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/errata01/csd01/pkcs11-curr-v3.0-errata01-csd01.pdf

Latest stage:
https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/errata01/pkcs11-curr-v3.0-errata01.docx (Authoritative)
https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/errata01/pkcs11-curr-v3.0-errata01.html
https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/errata01/pkcs11-curr-v3.0-errata01.pdf

Technical Committee:
OASIS PKCS 11 TC

Chairs:
Valerie Fenwick (vfenwick@apple.com), Apple, Inc.
Robert Relyea (rrelyea@redhat.com), Red Hat

Editors:
Dieter Bong (dieter.bong@utimaco.com), Utimaco IS GmbH
Tony Cox (tony.cox@tclogic.com.au), TC Logic

Additional artifacts:
This document is one component of a Work Product that also includes:

- PKCS #11 header files:
  https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/os/include/pkcs11-v3.0/
- Users of the standard can find the correct header files at https://github.com/oasis-tcs/pkcs11.

Related work:
This document provides Errata for:

- *PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 3.0*. Edited by Chris Zimman and Dieter Bong. 15 June 2020. OASIS Standard. https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/os/pkcs11-curr-v3.0-os.html.

This document is related to:

- *PKCS #11 Cryptographic Token Interface Profiles Version 3.0.* Edited by Tim Hudson. Latest stage. https://docs.oasis-open.org/pkcs11/pkcs11-profiles/v3.0/pkcs11-profiles-v3.0.html.
- *PKCS #11 Cryptographic Token Interface Base Specification Version 3.0.* Edited by Chris Zimman and Dieter Bong. Latest stage. https://docs.oasis-open.org/pkcs11/pkcs11-base/v3.0/pkcs11-base-v3.0.html.
- *PKCS #11 Cryptographic Token Interface Historical Mechanisms Specification Version 3.0*. Edited by Chris Zimman and Dieter Bong. Latest stage. https://docs.oasis-open.org/pkcs11/pkcs11-hist/v3.0/pkcs11-hist-v3.0.html.

Abstract:
This Errata document provides corrections to problematic items in the OASIS Standard *PKCS #11 Cryptographic Token Interface Current Mechanisms Version 3.0*.

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 stage" 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://groups.oasis-open.org/communities/tc-community-home2?CommunityKey=922ef643-1e10-4d65-a5ea-018dc7d3f0a4#technical.

TC members should send comments on this document to the TC's email list. Others should send comments to the OASIS public comment list as instructed here https://groups.oasis-open.org/communities/community-home?CommunityKey=05ce61d8-21dd-4bd1-bf18-018f5aa80127.

This document 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 document, 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).

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.

Key words:
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] and [RFC8174] when, and only when, they appear in all capitals, as shown here.

Citation format:
When referencing this document, the following citation format should be used:

[PKCS11-Current-v3.0-E01]

PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 3.0 Errata 01. Edited by Dieter Bong and Tony Cox. 31 January 2024. OASIS Committee Specification Draft 01. https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/errata01/csd01/pkcs11-curr-v3.0-errata01-cs01.html. Latest stage: https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/errata01/pkcs11-curr-v3.0-errata01.html.

Notices:

Table of Contents

1 Introduction

This document defines mechanisms that are anticipated to be used with the current version of PKCS #11. All text is normative unless otherwise labeled.

2 Errata for PKCS#11 Current Mechanisms Specification v3.0 OS

2.1 Modification of CKA_EC_Point for Edwards Elliptic Curve Public Key (2.3.5 Edwards Elliptic Curve public key objects)

Table 136, Edwards Elliptic Curve Public Key Object Attributes

Attribute	Data type	Meaning
CKA_EC_POINT[1,4]	Byte array	Public key bytes in little endian order as defined in RFC 8032

- Refer to [PKCS #11-Base] table 11 for footnotes

2.2 Modification of CKA_EC_Point for Edwards Elliptic Curve Private Key (2.3.6 Edwards Elliptic Curve private key objects)

Table 237, Edwards Elliptic Curve Private Key Object Attributes

Attribute	Data type	Meaning
CKA_VALUE[1,4,6,7]	Big integer	Private key bytes in little endian order as defined in RFC 8032

- Refer to [PKCS #11-Base] table 11 for footnotes

2.3 Modification of CKA_EC_Point for Montgomery Elliptic Curve Public Key (2.3.7 Montgomery Elliptic curve public key objects)

Table 338, Montgomery Elliptic Curve Public Key Object Attributes

Attribute	Data type	Meaning
CKA_EC_POINT[1,4]	Byte array	Public key bytes in little endian order as defined in RFC 7748

- Refer to [PKCS #11-Base] table 11 for footnotes

2.4 Modification of CKA_EC_Point for Montgomery Elliptic Curve Private Key (2.3.8 Montgomery Elliptic curve private key objects)

Table 439, Montgomery Elliptic Curve Private Key Object Attributes

Attribute	Data type	Meaning
CKA_VALUE[1,4,6,7]	Big integer	Private key bytes in little endian order as defined in RFC 7748

- Refer to [PKCS #11-Base] table 11 for footnotes

2.5 Modification of EC pPublicData Meaning (2.3.16 EC mechanisms parameters)

The fields of the structure have the following meanings:

pPublicData[1]	*pointer to other party's EC public key value. For short Weierstrass EC keys: a token MUST be able to accept this value encoded as a raw octet string (as per section A.5.2 of [ANSI X9.62]). A token MAY, in addition, support accepting this value as a DER-encoded ECPoint (as per section E.6 of [ANSI X9.62]) i.e. the same as a CKA_EC_POINT encoding. The calling application is responsible for converting the offered public key to the compressed or uncompressed forms of these encodings if the token does not support the offered form.* *For Montgomery keys: the public key is provided as bytes in little endian order as defined in RFC 7748.*

2.6 Clarification of Elliptic Curve Diffie-Hellman key derivation reference (2.3.17 Elliptic curve Diffie-Hellman key derivation)

The elliptic curve Diffie-Hellman (ECDH) key derivation mechanism, denoted **CKM_ECDH1_DERIVE**, is a mechanism for key derivation based on the Diffie-Hellman version of the elliptic curve key agreement scheme, as defined in ANSI X9.63 for ECDSA keys and RFC 7748 for Montgomery keys, where each party contributes one key pair all using the same EC domain parameters.

1 The encoding in V2.20 was not specified and resulted in different implementations choosing different encodings. Applications relying only on a V2.20 encoding (e.g. the DER variant) other than the one specified now (raw) may not work with all V2.30 compliant tokens.

3 PKCS #11 Implementation Conformance

PKCS #11 Implementation Conformance is defined in Section 3 of **[PKCS11-Curr]**.

Appendix A. References

This appendix contains the normative and informative references that are used in this document.

While any hyperlinks included in this appendix were valid at the time of publication, OASIS cannot guarantee their long-term validity.

A.1 Normative References

The following documents are referenced in such a way that some or all of their content constitutes requirements of this document.

[PKCS11-Curr]

PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 3.0. Edited by Chris Zimman and Dieter Bong. 15 June 2020. OASIS Standard. https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/os/pkcs11-curr-v3.0-os.html.

[RFC2119]

Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174]

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

A.2 Informative References

The following referenced documents are not required for the application of this document but may assist the reader with regard to a particular subject area.

[ANSI X9.62]

Accredited Standards Committee X9. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). 1998.

[ANSI X9.63]

Accredited Standards Committee X9. Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography. 2001.
URL: http://webstore.ansi.org/RecordDetail.aspx?sku=X9.63-2011

[RFC 7748]

Aboba et al, “Elliptic Curves for Security”, IETF RFC 7748, January 2016
URL: https://tools.ietf.org/html/rfc7748

[RFC 8032]

Aboba et al, “Edwards-Curve Digital Signature Algorithm (EdDSA)”, IETF RFC 8032, January 2017
URL: https://tools.ietf.org/html/rfc8032

Appendix B. Acknowledgments

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

Participants:

Warren Armstrong - QuintessenceLabs Pty Ltd.

Anthony Berglas - Cryptsoft Pty Ltd.

Dieter Bong - Utimaco IS GmbH

Roland Bramm - PrimeKey Solutions AB

Andrew Byrne - Dell

Hamish Cameron - nCipher

Kenli Chong - QuintessenceLabs Pty Ltd.

Justin Corlett - Cryptsoft Pty Ltd.

Tony Cox - Cryptsoft Pty Ltd.

Michele Drgon - Individual

Xuelei Fan - Oracle

Valerie Fenwick - Apple, Inc.

Jan Friedel - Oracle

Susan Gleeson - Oracle

Thomas Hardjono - M.I.T.

David Horton - Dell

Tim Hudson - Cryptsoft Pty Ltd.

Gershon Janssen - Individual

Jakub Jelen - Red Hat

Mark Joseph - P6R, Inc

Paul King - nCipher

Dina Kurktchi-Nimeh - Oracle

Philip Lafrance - ISARA Corporation

John Leiseboer - QuintessenceLabs Pty Ltd.

John Leser - Oracle

Chris Malafis - Red Hat

Michael Markowitz - Information Security Corporation

Chris Meyer - Utimaco IS GmbH

Daniel Minder - Utimaco IS GmbH

Darren Moffat - Oracle

Florian Poppa - QuintessenceLabs Pty Ltd.

Roland Reichenberg - Utimaco IS GmbH

Robert Relyea - Red Hat

Jonathan Schulze-Hewett - Information Security Corporation

Greg Scott - Cryptsoft Pty Ltd.

Martin Shannon - QuintessenceLabs Pty Ltd.

Oscar So - Individual

Patrick Steuer - IBM
Gerald Stueve - Fornetix
Jim Susoy - P6R, Inc
Sander Temme - nCipher
Manish Upasani - Utimaco IS GmbH
Charles White - Fornetix
Magda Zdunkiewicz - Cryptsoft Pty Ltd.

Appendix C. Revision History

Revision	Date	Editor	Changes Made
WD01	15 Nov 2021	Tony Cox	First draft of PKCS#11 Current Mechanisms v3.0 E01
WD02	16 Feb 2022	Dieter Bong	Fixed typo in section 2.6
WD03	10 Jan 2024	Dieter Bong	Section 2.5: Wording for pPublicData updated to match wording in PKCS#11 3.1 OASIS Standard

Appendix D. Notices

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: [https://www.oasis-open.org/policies-guidelines/ipr/].

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 AND ITS MEMBERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THIS DOCUMENT OR ANY PART THEREOF.

As stated in the OASIS IPR Policy, the following three paragraphs in brackets apply to OASIS Standards Final Deliverable documents (Committee Specifications, OASIS Standards, or Approved Errata).

[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 Standards Final Deliverable, 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 deliverable.]

[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 OASIS Standards Final Deliverable 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 OASIS Standards Final Deliverable. 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 OASIS Standards Final Deliverable 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 Standards Final Deliverable, 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 document, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, documents, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark/ for above guidance.