PKCS #11 Current Mechanisms Version 3.1

Working Draft 01

06 June 2019

Technical Committee:

[OASIS PKCS 11 TC](https://www.oasis-open.org/committees/pkcs11/)

Chairs:

Tony Cox ([tony.cox@cryptsoft.com](mailto:tony.cox@cryptsoft.com)), [Cryptsoft Pty Ltd](https://cryptsoft.com/)

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

Editors:

Dieter Bong ([dieter.bong@utimaco.com](mailto:dieter.bong@utimaco.com)), [Utimaco IS GmbH](https://hsm.utimaco.com/)

Tony Cox ([tony.cox@cryptsoft.com](mailto:tony.cox@cryptsoft.com)), [Cryptsoft Pty Ltd](https://cryptsoft.com/)

Additional artifacts:

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

* XML schemas: (list file names or directory name)
* Other parts (list titles and/or file names)
* (**Note:** Any normative computer language definitions that are part of the Work Product, such as XML instances, schemas and Java(TM) code, including fragments of such, must be (a) well formed and valid, (b) provided in separate plain text files, (c) referenced from the Work Product; and (d) where any definition in these separate files disagrees with the definition found in the specification, the definition in the separate file prevails. Remove this note before submitting for publication.)

Related work:

This specification replaces or supersedes:

* *PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40*. Edited by Susan Gleeson, Chris Zimman, Robert Griffin, and Tim Hudson. Latest version: <http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/pkcs11-curr-v2.40.html>.
* *PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 3.0*. Edited by Chris Zimman and Dieter Bong. Latest version: <https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.0/pkcs11-curr-v3.0.html>.

This specification is related to:

* Related specifications (hyperlink, if available)

Declared XML namespaces:

* list namespaces declared within this specification (hyperlink if HTTP-based)

Abstract:

This document defines mechanisms that are anticipated for use with the current version of PKCS #11.

Status:

This [Working Draft](https://www.oasis-open.org/policies-guidelines/oasis-defined-terms-2017-05-26#dWorkingDraft) (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or [approved](https://www.oasis-open.org/policies-guidelines/tc-process#committeeDraft) as a Committee Draft (Committee Specification Draft or a Committee Note Draft). The OASIS document [Approval Process](https://www.oasis-open.org/policies-guidelines/tc-process#standApprovProcess) begins officially with a TC vote to approve a WD as a Committee Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Draft.

This specification is provided under the [RF on RAND Terms](https://www.oasis-open.org/policies-guidelines/ipr#RF-on-RAND-Mode) Mode of the [OASIS IPR Policy](https://www.oasis-open.org/policies-guidelines/ipr), 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/pkcs11/ipr.php>).

Note that any machine-readable content ([Computer Language Definitions](https://www.oasis-open.org/policies-guidelines/tc-process#wpComponentsCompLang)) 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.

URI patterns:

Initial publication URI:  
https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.1/csprd01/pkcs11-curr-v3.1-csprd01.docx

Permanent "Latest version" URI:  
https://docs.oasis-open.org/pkcs11/pkcs11-curr/v3.1/pkcs11-curr-v3.1.docx

Copyright © OASIS Open 2019. 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](https://www.oasis-open.org/policies-guidelines/ipr) 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.

Table of Contents

[1 Introduction 4](#_Toc519870667)

[1.1 IPR Policy 4](#_Toc519870668)

[1.2 Terminology 4](#_Toc519870669)

[1.3 Normative References 4](#_Toc519870670)

[1.4 Non-Normative References 4](#_Toc519870671)

[2 Section Title 6](#_Toc519870672)

[2.1 Level 2 section title 6](#_Toc519870673)

[2.1.1 Level 3 section title 6](#_Toc519870674)

[2.1.1.1 Level 4 section title 6](#_Toc519870675)

[2.1.1.1.1 Level 5 6](#_Toc519870676)

[2.1.1.1.1.1 Level 6 6](#_Toc519870677)

[3 Security Considerations 7](#_Toc519870678)

[4 Conformance 8](#_Toc519870679)

[Appendix A. Acknowledgments 9](#_Toc519870680)

[Appendix B. Example Title 10](#_Toc519870681)

[B.1 Subsidiary section 10](#_Toc519870682)

[B.1.1 Sub-subsidiary section 10](#_Toc519870683)

[B.1.1.1 Sub-sub-subsidiary section 10](#_Toc519870684)

[B.1.1.1.1 Sub-sub-sub-subsidiary section 10](#_Toc519870685)

[Appendix C. Revision History 11](#_Toc519870686)

# Introduction

[All text is normative unless otherwise labeled]

## IPR Policy

This specification is provided under the [RF on RAND Terms](https://www.oasis-open.org/policies-guidelines/ipr#RF-on-RAND-Mode) Mode of the [OASIS IPR Policy](https://www.oasis-open.org/policies-guidelines/ipr), 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/pkcs11/ipr.php>).

## 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](#RFC2119)] and [[RFC8174](#RFC8174)] when, and only when, they appear in all capitals, as shown here.

## Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://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, <<http://www.rfc-editor.org/info/rfc8174>>.

[Reference] [Full reference citation]

## Non-Normative References

**[****RFC3552]** Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <<https://www.rfc-editor.org/info/rfc3552>>.

[Reference] [Full reference citation]

(**Note**: Each reference to a separate document or artifact in this work must be listed here and must be identified as either a Normative or a Non-Normative Reference.

*For all References – Normative and Non-Normative:*

Recommended approach: Set up [Reference] label elements as "Bookmarks", then create hyperlinks to them within the document. (**Here's how:** Insert hyperlink🡪Place in this document🡪scroll down to Bookmarks, select appropriate one.)

Use the "Ref term" and "Ref" paragraph styles to format references.

*The proper format for citation of technical work produced by an OASIS TC (whether Standards Track or Non-Standards Track) is:*

[Citation Label] Work Product [title](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#workProductName) (italicized). Edited by Albert Alston, Bob Ballston, and Calvin Carlson. Approval date (DD Month YYYY). OASIS [Stage](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#stage) Identifier and [Revision](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#revision) Number (*e.g.*, OASIS Committee Specification Draft 01). Principal URI ([version-specific URI](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#this-version), *e.g*., with stage component: somespec-v1.0-csd01.html). Latest version: ([latest version URI](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#latest-version), without stage identifiers).

For example:

**[OpenDoc-1.2]** *Open Document Format for Office Applications (OpenDocument) Version 1.2*. Edited by Patrick Durusau and Michael Brauer. 19 January 2011. OASIS Committee Specification Draft 07. <http://docs.oasis-open.org/office/v1.2/csd07/OpenDocument-v1.2-csd07.html>. Latest version: <http://docs.oasis-open.org/office/v1.2/OpenDocument-v1.2.html>.

*Reference sources:*

For references to **IETF RFCs**, use the approved citation formats at:  
<http://docs.oasis-open.org/templates/ietf-rfc-list/ietf-rfc-list.html>.

For references to **W3C Recommendations**, use the approved citation formats at:  
<http://docs.oasis-open.org/templates/w3c-recommendations-list/w3c-recommendations-list.html>.

Remove this note before submitting for publication.)

# Section Title

text

## Level 2 section title

text

### Level 3 section title

text

#### Level 4 section title

text

##### Level 5

Text

###### Level 6

Text

# Security Considerations

(**Note:** OASIS strongly recommends that Technical Committees consider issues that could affect security when implementing their specification and document them for implementers and adopters. For some purposes, you may find it required, e.g. if you apply for IANA registration.

While it may not be immediately obvious how your specification might make systems vulnerable to attack, most specifications, because they involve communications between systems, message formats, or system settings, open potential channels for exploit. For example, IETF [[RFC3552](#RFC3552)] lists “eavesdropping, replay, message insertion, deletion, modification, and man-in-the-middle” as well as potential denial of service attacks as threats that must be considered and, if appropriate, addressed in IETF RFCs.

In addition to considering and describing foreseeable risks, this section should include guidance on how implementers and adopters can protect against these risks.

We encourage editors and TC members concerned with this subject to read *Guidelines for Writing RFC Text on Security Considerations,* IETF [[RFC3552](#RFC3552)], for more information.)

# Conformance

(**Note**: The [OASIS TC Process](https://www.oasis-open.org/policies-guidelines/tc-process#wpComponentsConfClause) requires that a specification approved by the TC at the Committee Specification Public Review Draft, Committee Specification or OASIS Standard level must include a separate section, listing a set of numbered conformance clauses, to which any implementation of the specification must adhere in order to claim conformance to the specification (or any optional portion thereof). This is done by listing the conformance clauses here.

For the definition of "conformance clause," see [OASIS Defined Terms](https://www.oasis-open.org/policies-guidelines/oasis-defined-terms-2017-05-26#dConformanceClause).

See "Guidelines to Writing Conformance Clauses":   
<http://docs.oasis-open.org/templates/TCHandbook/ConformanceGuidelines.html>.

Remove this note before submitting for publication.)

1. Acknowledgments

(**Note:** A Work Product approved by the TC must include a list of people who participated in the development of the Work Product. This is generally done by collecting the list of names in this appendix. This list shall be initially compiled by the Chair, and any Member of the TC may add or remove their names from the list by request.

Remove this note before submitting for publication.)

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

Participants:

[Participant Name, Affiliation | Individual Member]

[Participant Name, Affiliation | Individual Member]

1. Example Title

text

* 1. Subsidiary section

text

* + 1. Sub-subsidiary section

Text

* + - 1. Sub-sub-subsidiary section

text

* + - * 1. Sub-sub-sub-subsidiary section

text

1. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| [Rev number] | [Rev Date] | [Modified By] | [Summary of Changes] |