Published on *OASIS* (https://www.oasis-open.org)

15-day Public Review for #PKCS11 Committee Specification and Committee Note Drafts

Submitted by censign on Fri, 2014-05-16 16:38
Type:
Public Review

The OASIS PKCS 11 TC [1] members have recently approved four Committee Specification Drafts (CSD) and one Committee Note Draft (CND) and submitted these for 15-day public review:

PKCS #11 Cryptographic Token Interface Base Specification Version 2.40
Committee Specification Draft 02 / Public Review Draft 02
07 May 2014

PKCS #11 Cryptographic Token Interface Current Mechanisms Specification
Version 2.40
Committee Specification Draft 02 / Public Review Draft 02
23 April 2014

PKCS #11 Cryptographic Token Interface Historical Mechanisms Specification
Version 2.40
Committee Specification Draft 02 / Public Review Draft 02
23 April 2014

PKCS #11 Cryptographic Token Interface Profiles Version 2.40
Committee Specification Draft 02 / Public Review Draft 02
23 April 2014

PKCS #11 Cryptographic Token Interface Usage Guide Version 2.40
Committee Note Draft 02 / Public Review Draft 02
23 April 2014

With these releases we are testing a convenience option for submitting comments to the Technical Committee. Please see the details under ?Public Review Period? below.

Specification Overview:

The PKCS #11 Base Specification provides normative definition of PKCS #11 objections, attributes and operations.

The PKCS #11 Current Mechanisms document describes the application of PKCS #11 objects, attributes and

operations for specific mechanisms currently in general use.

The PKCS #11 Historical Mechanisms document describes the application of PKCS #11 objects, attributes and operations for specific mechanisms that have been but are no longer in general use.

The PKCS #11 Profiles document describes conformant profiles consisting PKCS #11 objects, attributes, operations and mechanisms.

The PKCS #11 Cryptographic Token Interface Usage Guide provides guidance on using PKCS #11 v2.40.

TC Description:

The OASIS PKCS 11 Technical Committee develops enhancements to improve the PKCS #11 standard for ease of use in code libraries, open source applications, wrappers, and enterprise/COTS products: implementation guidelines, usage tutorials, test scenarios and test suites, interoperability testing, coordination of functional testing, development of conformance profiles, and providing reference implementations.

Public Review Period:

The public review starts 19 May 2014 at 00:00 GMT and ends 01 June 2014 at 23:59 GMT.

These drafts were previously submitted for public review [2]. This 15-day review is limited in scope to changes made from the previous review. Changes are highlighted in the diff-marked PDF files [3].

This is an open invitation to comment. OASIS solicits feedback from potential users, developers and others, whether OASIS members or not, for the sake of improving the interoperability and quality of its technical work.

With this public review, we are testing a new convenience feature for sending comments to the Technical Committee. The files:

http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/csprd02/pkcs11-base-... [1]

http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/csprd02/pkcs11-curr-... [2]

http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/csprd02/pkcs11-hist-... [3]

http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-p... [4]

http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cnprd02/pkcs11-ug-v2.4... [5]

contain the HTML versions of the drafts with a ?[comment?]? link next to each section heading. Clicking on this link will launch your email application and begin a message to pkcs11-comment@lists.oasis-open.org [6] with the specific section number and title in the subject line. (For example, ?Public review comment for pkcs11-curr-v2.40-csprd02: 1.1 References?) Simply enter your comment and click send.

You must be subscribed to the pkcs11-comment@lists.oasis-open.org [6] mailing list in order to send your comments. Instructions on how to subscribe can be found at https://www.oasis-open.org/committees/comments/index.php?wg_abbrev=pkcs11 [7].

Note that the Table of Contents doesn?t work in this version and other internal document links may not work in these files. That is one of the items we need fix before making this capability more broadly available. Please feel free to let us know if you find this feature helpful. We plan to refine it and make it a part of our normal public

review process.

URIs:

The prose specification document and related files are available here:

- PKCS #11 Cryptographic Token Interface Base Specification

Editable Source (Authoritative):
http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/csprd02/pkcs11-base-... [8]

HTML:
http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/csprd02/pkcs11-base-... [9]

PDF:
http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/csprd02/pkcs11-base-... [10]

ZIP distribution file (complete):
http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/csprd02/pkcs11-base-... [11]

- PKCS #11 Cryptographic Token Interface Current Mechanisms Specification

Editable Source (Authoritative):
http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/csprd02/pkcs11-curr-... [12]

HTML:
http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/csprd02/pkcs11-curr-... [13]

PDF:
http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/csprd02/pkcs11-curr-... [14]

ZIP distribution file (complete):
http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/csprd02/pkcs11-curr-... [15]

-PKCS #11 Cryptographic Token Interface Historical Mechanisms Specification

Editable Source (Authoritative):
http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/csprd02/pkcs11-hist-... [16]

HTML:
http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/csprd02/pkcs11-hist-... [17]

PDF:
http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/csprd02/pkcs11-hist-... [18]

ZIP distribution file (complete):
http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/csprd02/pkcs11-hist-... [19]

- PKCS #11 Cryptographic Token Interface Profiles

Editable Source (Authoritative):
http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-p... [20]

HTML:
http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-p... [21]

PDF:
http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-p... [22]

ZIP distribution file (complete):
http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-p... [23]

- PKCS #11 Cryptographic Token Interface Usage Guide

Editable Source (Authoritative):
http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cnprd02/pkcs11-ug-v2.4... [24]

HTML:
http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cnprd02/pkcs11-ug-v2.4... [25]

PDF:
http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cnprd02/pkcs11-ug-v2.4... [26]

ZIP distribution file (complete):
http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cnprd02/pkcs11-ug-v2.4... [27]

Additional information about the specification and the OASIS PKCS 11 TC can be found at the TC's public home page:

https://www.oasis-open.org/committees/pkcs11/ [28]

Comments may be submitted to the TC by any person through the use of the OASIS TC Comment Facility which can be used by following the instructions on the TC's "Send A Comment" page, or directly at:

https://www.oasis-open.org/committees/comments/index.php?wg_abbrev=pkcs11 [7]

Comments submitted by TC non-members for this work and for other work of this TC are publicly archived and can be viewed at:

https://lists.oasis-open.org/archives/pkcs-comment/ [29]

All comments submitted to OASIS are subject to the OASIS Feedback License, which ensures that the feedback you provide carries the same obligations at least as the obligations of the TC members. In connection with this public review of the PKCS 11 Committee Specification and Note Drafts, we call your attention to the OASIS IPR Policy [4] applicable especially [5] to the work of this technical committee. All members of the TC should be familiar with
this document, which may create obligations regarding the disclosure and availability of a member's patent, copyright, trademark and license rights that read on an approved OASIS specification.

OASIS invites any persons who know of any such claims to disclose these if they may be essential to the implementation of the above specification, so that notice of them may be posted to the notice page for this TC's

work.

========== Additional references:

[1] OASIS PKCS 11 TC
http://www.oasis-open.org/committees/pkcs11/ [30]

[2] Previous public review:
- 30-day public review, 25 November 2013: https://lists.oasis-open.org/archives/tc-announce/201311/msg00012.html [31]
- Comment resolution log (one common log, copy in each csprd01 directory):
http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/csprd01/pkcs11-v2.40... [32]

[3] Redlined DIFF files:

- Base: http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/csprd02/pkcs11-base-... [33]

- Curr: http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/csprd02/pkcs11-curr-... [34]

- Hist: http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/csprd02/pkcs11-hist-... [35]

- Profiles: http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-p... [36]

- Usage guide: http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cnprd02/pkcs11-ug-v2.4... [37]

[4] http://www.oasis-open.org/who/intellectualproperty.php [38]

[5] http://www.oasis-open.org/committees/pkcs11/ipr.php [39]
https://www.oasis-open.org/policies-guidelines/ipr#s10.2.2 [40]
RF on RAND Mode

Associated TC:
PKCS 11
Deadline:
Mon, 2014-05-19 - Mon, 2014-06-02

Links:
[1] http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/csprd02/pkcs11-base-v2.40-csprd02-COMMENT-TAGS.html
[2] http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/csprd02/pkcs11-curr-v2.40-csprd02-COMMENT-TAGS.html
[3] http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/csprd02/pkcs11-hist-v2.40-csprd02-COMMENT-TAGS.html
[4] http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-profiles-v2.40-csprd02-COMMENT-TAGS.html
[5] http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cnprd02/pkcs11-ug-v2.40-cnprd02-COMMENT-TAGS.html
[6] mailto:pkcs11-comment@lists.oasis-open.org
[7] https://www.oasis-open.org/committees/comments/index.php?wg_abbrev=pkcs11
[8] http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/csprd02/pkcs11-base-v2.40-csprd02.doc
[9] http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/csprd02/pkcs11-base-v2.40-csprd02.html

[10] http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/csprd02/pkcs11-base-v2.40-csprd02.pdf
[11] http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/csprd02/pkcs11-base-v2.40-csprd02.zip
[12] http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/csprd02/pkcs11-curr-v2.40-csprd02.doc
[13] http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/csprd02/pkcs11-curr-v2.40-csprd02.html
[14] http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/csprd02/pkcs11-curr-v2.40-csprd02.pdf
[15] http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/csprd02/pkcs11-curr-v2.40-csprd02.zip
[16] http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/csprd02/pkcs11-hist-v2.40-csprd02.doc
[17] http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/csprd02/pkcs11-hist-v2.40-csprd02.html
[18] http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/csprd02/pkcs11-hist-v2.40-csprd02.pdf
[19] http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/csprd02/pkcs11-hist-v2.40-csprd02.zip
[20] http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-profiles-v2.40-csprd02.doc
[21] http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-profiles-v2.40-csprd02.html
[22] http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-profiles-v2.40-csprd02.pdf
[23] http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-profiles-v2.40-csprd02.zip
[24] http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cnprd02/pkcs11-ug-v2.40-cnprd02.doc
[25] http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cnprd02/pkcs11-ug-v2.40-cnprd02.html
[26] http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cnprd02/pkcs11-ug-v2.40-cnprd02.pdf
[27] http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cnprd02/pkcs11-ug-v2.40-cnprd02.zip
[28] https://www.oasis-open.org/committees/pkcs11/
[29] https://lists.oasis-open.org/archives/pkcs-comment/
[30] http://www.oasis-open.org/committees/pkcs11/
[31] https://lists.oasis-open.org/archives/tc-announce/201311/msg00012.html
[32] http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/csprd01/pkcs11-v2.40-csprd01-comment-resolution-log.xls
[33] http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/csprd02/pkcs11-base-v2.40-csprd02-diff.pdf
[34] http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/csprd02/pkcs11-curr-v2.40-csprd02-diff.pdf
[35] http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/csprd02/pkcs11-hist-v2.40-csprd02-diff.pdf
[36] http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-profiles-v2.40-csprd02-diff.pdf
[37] http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cnprd02/pkcs11-ug-v2.40-cnprd02-diff.pdf
[38] http://www.oasis-open.org/who/intellectualproperty.php
[39] http://www.oasis-open.org/committees/pkcs11/ipr.php
[40] https://www.oasis-open.org/policies-guidelines/ipr#s10.2.2