



PKCS #11 Cryptographic Token Interface Profiles Version 2.40

Committee Specification Draft ~~0102~~ /
Public Review Draft ~~0102~~

~~30 October 2013~~

23 April 2014

Specification URIs

This version:

<http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-profiles-v2.40-csprd02.doc> ([Authoritative](#))
<http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-profiles-v2.40-csprd02.html>
<http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-profiles-v2.40-csprd02.pdf>

Previous version:

<http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd01/pkcs11-profiles-v2.40-csprd01.doc> (Authoritative)
<http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd01/pkcs11-profiles-v2.40-csprd01.html>
<http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd01/pkcs11-profiles-v2.40-csprd01.pdf>

~~Previous version:~~

~~N/A~~

Latest version:

<http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/pkcs11-profiles-v2.40.doc> (Authoritative)
<http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/pkcs11-profiles-v2.40.html>
<http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/pkcs11-profiles-v2.40.pdf>

Technical Committee:

OASIS PKCS 11 TC

Chairs:

Robert Griffin (robert.griffin@rsa.com), EMC Corporation
Valerie Fenwick (valerie.fenwick@oracle.com), Oracle

Editor:

Tim Hudson (tjh@cryptsoft.com), Cryptsoft Pty Ltd.

Related work:

This specification is related to:

- *PKCS #11 Cryptographic Token Interface Base Specification Version 2.40*. Edited by [Susan Gleeson and Chris Zimman](#). Latest version. <http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/pkcs11-base-v2.40.html>.

- *PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40.* Edited by [Susan Gleeson and Chris Zimman](#). Latest version. <http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/pkcs11-curr-v2.40.html>.
- *PKCS #11 Cryptographic Token Interface Historical Mechanisms Specification Version 2.40.* Edited by [Susan Gleeson and Chris Zimman](#). Latest version. <http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/pkcs11-hist-v2.40.html>.
- *PKCS #11 Cryptographic Token Interface Usage Guide Version 2.40.* Edited by [John Leiseboer and Robert Griffin](#). Latest version. <http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/pkcs11-ug-v2.40.html>.

Abstract:

This document is intended for developers and architects who wish to design systems and applications that conform to the PKCS #11 Cryptographic Token Interface ~~specification~~standard.

The PKCS #11 Cryptographic Token Interface ~~specification~~ standard documents an API for devices that may hold cryptographic information and may perform cryptographic functions.

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.

Technical Committee members should send comments on this specification to the Technical Committee’s email list. Others should send comments to the Technical Committee by using the “Send A Comment” button on the Technical Committee’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 Technical Committee 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-profilesProfiles-v2.40]

PKCS #11 Cryptographic Token Interface Profiles Version 2.40. ~~30 October 2013.~~ Edited by [Tim Hudson](#). [23 April 2014](#). OASIS Committee Specification Draft ~~0402~~ / Public Review Draft ~~04-02~~. <http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/csprd02/pkcs11-profiles-v2.40-csprd02.html>. Latest version: <http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/pkcs11-profiles-v2.40.html>.

Notices

Copyright © OASIS Open 2013~~4~~. 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	Description of this Document.....	5
1.2	Terminology.....	5
1.3	Normative References.....	5
1.4	Non-Normative References.....	6
2	Profiles.....	7
2.1	PKCS #11 Profiles.....	7
2.2	Guidelines for Specifying Conformance Clauses.....	7
2.3	Guidelines for Validating Conformance to PKCS #11 Profiles.....	7
3	Conformance.....	8
3.1	Purpose of this Section.....	8
3.2	Baseline Consumer Clause.....	8
3.2.1	Implementation Conformance.....	8
3.2.2	Conformance of a PKCS #11 Baseline Consumer.....	8
3.3	Baseline Provider Clause.....	9
3.3.1	Implementation Conformance.....	9
3.3.2	Conformance of a PKCS #11 Baseline Provider.....	9
3.4	Extended Consumer Clause.....	10
3.4.1	Implementation Conformance.....	10
3.4.2	Conformance of a PKCS #11 Extended Consumer.....	10
3.5	Extended Provider Clause.....	12
3.5.1	Implementation Conformance.....	12
3.5.2	Conformance of a PKCS #11 Extended Provider.....	12
3.6	Authentication Token Clause.....	13
3.6.1	Implementation Conformance.....	13
3.6.2	Conformance of a Authentication Token.....	13
Appendix A.	Acknowledgments.....	14
Appendix B.	Revision History.....	16

1 Introduction

1.1 Description of this Document

OASIS requires a conformance section in an approved committee specification ([PKCS11-~~SPEC~~Base] [TCPROC], section 2.18 Work Product Quality, paragraph 8a):

A specification that is approved by the TC at the 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 document intends to meet this OASIS requirement on conformance clauses for providers and consumers of cryptographic services via PKCS #11 ([PKCS11-~~(PKCS11-SPEC-Base)~~] Section 6 (PKCS#11 Implementation Conformance) through profiles that define the use of ~~PKCS11~~PKCS #11 data types, objects, functions and mechanisms within specific contexts of provider and consumer interaction. These profiles define a set of normative constraints for employing ~~PKCS11~~PKCS #11 within a particular environment or context of use. They may, optionally, require the use of specific ~~PKCS11~~PKCS #11 functionality or in other respects define the processing rules to be followed by profile actors.

For normative definition of the elements of ~~PKCS11~~PKCS #11 specified in these profiles, see the PKCS #11 Cryptographic Token Interface Base Specification ([PKCS11-~~SPEC~~Base]).and the PKCS #11 Cryptographic Token Interface Current Mechanisms ([PKCS11-~~CMECH~~Curr]). Illustrative guidance for the implementation of providers and consumers of ~~PKCS11~~PKCS #11 is provided in the PKCS #11 Cryptographic Token Interface Usage Guide ([PKCS11-UG]).

1.1.2 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].

1.2.1.3 Normative References

~~[PKCS11-Base]~~ PKCS #11 Cryptographic Token Interface Base Specification Version 2.40 <<DATE>>. OASIS Working Draft, <http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/pkcs11-base-v2.40.html>~~CMECH~~.

~~[PKCS11-Curr]~~ PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version <<VERSION>>.2.40 <<DATE>>. OASIS Working Draft, [<<URI>>](http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/pkcs11-curr-v2.40.html).

~~[PKCS11-HMECHHist]~~ PKCS #11 Cryptographic Token Interface Historical Mechanisms Specification Version <<VERSION>>. <<DATE>>, OASIS Working Draft, [<<URI>>](http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/pkcs11-hist-v2.40.html)

~~[PKCS11-SPEC]~~ PKCS #11 Cryptographic Token Interface Base Specification Version <<VERSION>>. <<DATE>>. OASIS Working Draft, <<URI>>

[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>.

[TCPROC] OASIS, *Technical Committee (TC) Process, Version 31 January 2013*, 31 January 2013, <https://www.oasis-open.org/policies-guidelines/tc-process>.

44 | **1.31.4 Non-Normative References**

45 | **[PKCS11-UG]** *PKCS #11 Cryptographic Token Interface Usage Guide Specification Version*
46 | ~~<<VERSION>>~~2.40 <<DATE>>. OASIS Working Draft, [http://docs.oasis-](http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/pkcs11-ug-v2.40.html)
47 | [open.org/pkcs11/pkcs11-ug/v2.40/pkcs11-ug-v2.40.html](http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/pkcs11-ug-v2.40.html)~~<<URI>>~~
48 |

49 2 Profiles

50 2.1 PKCS #11 Profiles

51 This document defines a selected set of conformance clauses which form PKCS#11PKCS #11 Profiles.
52 The PKCS#11PKCS 11 TC also welcomes proposals for new profiles. PKCS#11PKCS 11 TC members are
53 encouraged to submit these proposals to the PKCS#11PKCS 11 TC for consideration for inclusion in a
54 future version of this TC-approved document. However, some OASIS members ~~may~~MAY simply wish to
55 inform the committee of profiles or other work related to PKCS#11PKCS #11.

56 ~~2.12.2~~ Guidelines for Specifying Conformance Clauses

57 This section provides a checklist of issues that SHALL be addressed by each clause.

- 58 | 1. Implement functionality as mandated by [PKCS11-SPECBase] **Section 6** (PKCS#11
59 Implementation Conformance)
- 60 | 2. Specify the list of additional data types that SHALL be supported
- 61 | 3. Specify the list of additional objects that SHALL be supported
- 62 | 4. Specify the list of additional functions that SHALL be supported
- 63 | 5. Specify the list of additional mechanisms that SHALL be supported

65 | ~~2.22.3~~ Guidelines for Validating Conformance to PKCS#11PKCS #11 66 Profiles

67 | A PKCS#11PKCS #11 provider implementation SHALL claim conformance to a specific provider profile
68 only if it instruments all required data types, objects, functions and mechanisms of that profile

- 69 • All data types specified as required in that profile
- 70 • All objects specified as required in that profile
- 71 • All functions specified as required in that profile
- 72 • All mechanisms specified as required in that profile

73 | A PKCS#11PKCS #11 consumer implementation SHALL claim conformance to a specific consumer
74 profile only if it instruments all required data types, objects, functions and mechanisms of that profile

- 75 • All data types specified as required in that profile
- 76 • All objects specified as required in that profile
- 77 • All functions specified as required in that profile
- 78 • All mechanisms specified as required in that profile

79

80 3 Conformance

81 3.1 Purpose of this Section

82 The following subsections describe currently-defined profiles related to the use of PKCS11PKCS #11.
83 The profiles define classes of PKCS #11 functionality to which an implementation can declare
84 conformance.

85 3.1.3.2 Baseline Consumer Clause

86 This profile builds on the Baseline ProviPKCS11A PKCS #11 consumer conformance clauses to provide
87 somecalls a PKCS #11 provider implementation of the PKCS #11 API in order to use the cryptographic
88 functionality from that provider.

89
90 This profile specifies the most basic functionality that would be expected of a conformant PKCS11PKCS
91 #11 consumer – the ability to consume information via the cryptographic services offered by a provider.

92 3.1.13.2.1 Implementation Conformance

93 An implementation is a conforming Baseline Consumer Clause if it meets the conditions as outlined in the
94 following section.

95 3.1.23.2.2 Conformance of a PKCS11PKCS #11 Baseline Consumer

96 An implementation conforms to this specification as a Baseline Consumer if it meets the following
97 conditions:

- 98 1. Supports the conditions required by the PKCS11PKCS #11 conformance clauses ([PKCS11-
99 SPECBase] Section 6 (PKCS#11 Implementation Conformance))
- 100 2. Supports the following data types:
 - 101 a. CK_VERSION ([PKCS11-SPECBase] 3.1)
 - 102 b. CK_INFO ([PKCS11-SPECBase] 3.1)
 - 103 c. CK_SLOT_ID ([PKCS11-SPECBase] 3.2)
 - 104 d. CK_SLOT_INFO ([PKCS11-SPECBase] 3.2)
 - 105 e. CK_TOKEN_INFO ([PKCS11-SPECBase] 3.2)
 - 106 f. CK_SESSION_HANDLE ([PKCS11-SPECBase] 3.3)
 - 107 g. CK_USER_TYPE ([PKCS11-SPECBase] 3.3)
 - 108 h. CK_SESSION_INFO ([PKCS11-SPECBase] 3.3)
 - 109 i. CK_OBJECT_HANDLE ([PKCS11-SPECBase] 3.4)
 - 110 j. CK_OBJECT_CLASS ([PKCS11-SPECBase] 3.4)
 - 111 k. CK_ATTRIBUTE_TYPE ([PKCS11-SPECBase] 3.4)
 - 112 l. CK_ATTRIBUTE ([PKCS11-SPECBase] 3.4)
 - 113 m. CK_RV ([PKCS11-SPECBase] 3.6)
 - 114 n. CK_FUNCTION_LIST ([PKCS11-SPECBase] 3.6)
 - 115 o. CK_C_INITIALIZE_ARGS ([PKCS11-SPECBase] 3.7)
- 116 3. Supports the following objects:
 - 117 a. CKA_CLASS ([PKCS11-SPECBase] 4.2)
 - 118 b. CKA_VALUE ([PKCS11-SPECBase])
- 119 4. Supports the following functions:
 - 120 a. C_GetFunctionList ([PKCS11-SPECBase] 5.4)
 - 121 b. C_Initialize ([PKCS11-SPECBase] 5.4)
 - 122 c. C_Finalize ([PKCS11-SPECBase] 5.4)

- d. C_GetInfo ([PKCS11-~~SPECBase~~] 5.4)
 - e. C_GetSlotList ([PKCS11-~~SPECBase~~] 5.5)
 - f. C_GetSlotInfo ([PKCS11-~~SPECBase~~] 5.5)
 - g. C_GetTokenInfo ([PKCS11-~~SPECBase~~] 5.5)
 - h. C_OpenSession ([PKCS11-~~SPECBase~~] 5.6)
 - i. C_CloseSession ([PKCS11-~~SPECBase~~] 5.6)
5. Supports the following mechanisms:
- a. None specified
6. Supports Error Handling ([PKCS11-~~SPECBase~~] 5.1) for any supported object, function or mechanism
7. Optionally supports any clause within [PKCS11-~~SPECBase~~] that is not listed above
8. Optionally supports extensions outside the scope of this standard (e.g., vendor defined extensions, conformance clauses) that do not contradict any ~~PKCS11~~PKCS #11 requirements

136 ~~3-23.3~~ **Baseline Provider Clause**

137 ~~This profile builds on the PKCS11A PKCS #11 provider conformance clauses~~makes cryptographic
 138 functionality available to provide some a consuming application in terms of the PKCS #11 API.
 139 This profile specifies the most basic functionality that would be expected of a conformant ~~PKCS11~~PKCS
 140 #11 provider – the ability to provide information about the capabilities of the cryptographic services
 141 provided.

142 ~~3-2-13.3.1~~ **Implementation Conformance**

143 An implementation is a conforming Baseline Provider ~~Clause~~ if it meets the conditions as outlined in the
 144 following section.

145 ~~3-2-23.3.2~~ **Conformance of a ~~PKCS11~~PKCS #11 Baseline Provider**

146 An implementation conforms to this specification as a Baseline Provider if it meets the following
 147 conditions:

- 148 1. Supports the conditions required by the PKCS #11 conformance clauses ([PKCS11-Base]
 149 Section 6 (PKCS#11 Implementation Conformance)
- 150 2. Supports the following data types:
 - 151 a. CK_VERSION ([PKCS11-Base] 3.1)
 - 152 b. CK_INFO ([PKCS11-Base] 3.1)
 - 153 c. CK_SLOT_ID ([PKCS11-Base] 3.2)
 - 154 d. CK_SLOT_INFO ([PKCS11-Base] 3.2)
 - 155 e. CK_TOKEN_INFO ([PKCS11-Base] 3.2)
 - 156 f. CK_SESSION_HANDLE ([PKCS11-Base] 3.3)
 - 157 g. CK_USER_TYPE ([PKCS11-Base] 3.3)
 - 158 h. CK_SESSION_INFO ([PKCS11-Base] 3.3)
 - 159 i. CK_OBJECT_HANDLE ([PKCS11-Base] 3.4)
 - 160 j. CK_OBJECT_CLASS ([PKCS11-Base] 3.4)
 - 161 k. CK_ATTRIBUTE_TYPE ([PKCS11-Base] 3.4)
 - 162 l. CK_ATTRIBUTE ([PKCS11-Base] 3.4)
 - 163 m. CK_RV ([PKCS11-Base] 3.6)
 - 164 n. CK_FUNCTION_LIST ([PKCS11-Base] 3.6)
 - 165 o. CK_C_INITIALIZE_ARGS ([PKCS11-Base] 3.7)
- 166 3. Supports the following objects:
 - 167 a. CKA_CLASS ([PKCS11-Base] 4.2)
 - 168 b. CKA_TOKEN ([PKCS11-Base] 4.2)
 - 169 c. CKA_VALUE ([PKCS11-Base])
 - 170 d. CKA_ID ([PKCS11-Base])

- 171 e. CKA_PRIVATE ([PKCS11-Base] x.y)
- 172 f. CKA_MODIFIABLE ([PKCS11-Base])
- 173 g. CKA_LABEL ([PKCS11-Base])
- 174 4. Supports the following functions:
- 175 a. C_GetFunctionList ([PKCS11-Base] 5.4)
- 176 b. C_Initialize ([PKCS11-Base] 5.4)
- 177 c. C_Finalize ([PKCS11-Base] 5.4)
- 178 d. C_GetInfo ([PKCS11-Base] 5.4)
- 179 e. C_GetSlotList ([PKCS11-Base] 5.5)
- 180 f. C_GetSlotInfo ([PKCS11-Base] 5.5)
- 181 g. C_GetTokenInfo ([PKCS11-Base] 5.5)
- 182 h. C_OpenSession ([PKCS11-Base] 5.6)
- 183 i. C_CloseSession ([PKCS11-Base] 5.6)
- 184 j. C_GetSessionInfo ([PKCS11-Base] 5.6)
- 185 k. C_FindObjectsInit ([PKCS11-Base] 5.6)
- 186 l. C_FindObjects ([PKCS11-Base] 5.6)
- 187 m. C_FindObjectsFinal ([PKCS11-Base] 5.6)
- 188 n. C_GetAttributeValue ([PKCS11-Base] 5.7)

189 5. Supports the following mechanisms:

- 190 a. None specified
- 191 6. Supports Error Handling ([PKCS11-Base] 5.1) for any supported object, function or mechanism
- 192 7. Optionally supports any clause within [PKCS11-Base] that is not listed above
- 193 8. Optionally supports extensions outside the scope of this standard (e.g., vendor defined
- 194 extensions, conformance clauses) that do not contradict any PKCS #11 requirements

195 3.4 Extended Consumer Clause

196 This profile builds on the PKCS#11 Baseline Consumer profile to add support for mechanism-based
 197 usage.

198 3.4.1 Implementation Conformance

199 An implementation is a conforming Extended Consumer if it meets the conditions as outlined in the
 200 following section.

201 3.4.2 Conformance of a PKCS #11 Extended Consumer

202 An implementation conforms to this specification as Extended Consumer if it meets the following
 203 conditions:

- 204 1. Supports the conditions required by the PKCS11 conformance clauses ([PKCS11-SPEC] Section
- 205 6 (PKCS#11 Implementation Conformance))

206 ~~2.1. Base~~ Supports the following data types:

- 207 ~~a. CK_VERSION ([PKCS11-SPEC] 3.1)~~
- 208 ~~b. CK_INFO ([PKCS11-SPEC] 3.1)~~
- 209 ~~c. CK_SLOT_ID ([PKCS11-SPEC] 3.2)~~
- 210 ~~d. CK_SLOT_INFO ([PKCS11-SPEC] 3.2)~~
- 211 ~~e. CK_TOKEN_INFO ([PKCS11-SPEC] 3.2)~~
- 212 ~~f. CK_SESSION_HANDLE ([PKCS11-SPEC] 3.3)~~
- 213 ~~g. CK_USER_TYPE ([PKCS11-SPEC] 3.3)~~
- 214 ~~h. CK_SESSION_INFO ([PKCS11-SPEC] 3.3)~~
- 215 ~~i. CK_OBJECT_HANDLE ([PKCS11-SPEC] 3.4)~~
- 216 ~~j. CK_OBJECT_CLASS ([PKCS11-SPEC] 3.4)~~
- 217 ~~k. CK_ATTRIBUTE_TYPE ([PKCS11-SPEC] 3.4)~~
- 218 ~~l. CK_ATTRIBUTE ([PKCS11-SPEC] 3.4)~~

- 219 m. ~~CK_RV ([PKCS11-SPEC] 3.6)~~
- 220 n. ~~CK_FUNCTION_LIST ([PKCS11-SPEC] 3.6)~~
- 221 o. ~~CK_C_INITIALIZE_ARGS ([PKCS11-SPEC] 3.7)~~

222 ~~3. Supports the following objects:~~

- 223 a. ~~CKA_CLASS ([PKCS11-SPEC] 4.2)~~
- 224 b. ~~CKA_TOKEN ([PKCS11-SPEC] 4.2)~~
- 225 c. ~~CKA_VALUE ([PKCS11-SPEC])~~
- 226 d. ~~CKA_ID ([PKCS11-SPEC])~~
- 227 e. ~~CKA_PRIVATE ([PKCS11-SPEC] x.y)~~
- 228 f. ~~CKA_MODIFIABLE ([PKCS11-SPEC])~~
- 229 g. ~~CKA_LABEL ([PKCS11-SPEC])~~

230 ~~4. Supports the following functions:~~

- 231 a. ~~C_GetFunctionList ([PKCS11-SPEC] 5.4)~~
- 232 b. ~~C_Initialize ([PKCS11-SPEC] 5.4)~~
- 233 c. ~~C_Finalize ([PKCS11-SPEC] 5.4)~~
- 234 d. ~~C_GetInfo ([PKCS11-SPEC] 5.4)~~
- 235 e. ~~C_GetSlotList ([PKCS11-SPEC] 5.5)~~
- 236 f. ~~C_GetSlotInfo ([PKCS11-SPEC] 5.5)~~
- 237 g. ~~C_GetTokenInfo ([PKCS11-SPEC] 5.5)~~
- 238 h. ~~C_OpenSession ([PKCS11-SPEC] 5.6)~~
- 239 i. ~~C_CloseSession ([PKCS11-SPEC] 5.6)~~
- 240 j. ~~C_GetSessionInfo ([PKCS11-SPEC] 5.6)~~
- 241 k. ~~C_FindObjectsInit ([PKCS11-SPEC] 5.6)~~
- 242 l. ~~C_FindObjects ([PKCS11-SPEC] 5.6)~~
- 243 m. ~~C_FindObjectsFinal ([PKCS11-SPEC] 5.6)~~
- 244 n. ~~C_GetAttributeValue ([PKCS11-SPEC] 5.7)~~

245 ~~5. Supports the following mechanisms:~~

- 246 a. ~~None specified~~
- 247 ~~6. Supports Error Handling ([PKCS11-SPEC] 5.1) for any supported object, function or mechanism~~
- 248 ~~7. Optionally supports any clause within [PKCS11-SPEC] that is not listed above~~
- 249 ~~8. Optionally supports extensions outside the scope of this standard (e.g., vendor defined~~
- 250 ~~extensions, conformance clauses) that do not contradict any PKCS11 requirements~~

251 ~~3.31.1 Extended Consumer Clause~~

252 ~~This profile builds on the baseline consumer clause to add support for mechanism based usage.~~

253 ~~3.3.11.1.1 Implementation Conformance~~

254 ~~An implementation is a conforming Extended Consumer Clause if it meets the conditions as outlined in~~

255 ~~the following section.~~

256 ~~3.3.2 Conformance of a PKCS11 Extended Provider~~

257 ~~An implementation conforms to this specification as Extended Provider if it meets the following conditions:~~

- 258 1. ~~Supports the conditions required by the PKCS11 conformance clauses ([PKCS11-SPEC] Section~~
- 259 ~~6 (PKCS#11 Implementation Conformance)~~
- 260 2. ~~Supports the conditions required by the PKCS11 Baseline Consumer clauses section 3.2~~
- 261 3. ~~Supports the following additional data types:~~
 - 262 a. ~~CK_MECHANISM_TYPE ([PKCS11-SPECBase] 3.4)~~
 - 263 b. ~~CK_MECHANISM ([PKCS11-SPECBase] 3.4)~~
- 264 4. ~~Supports the following additional objects:~~

- 265 a. None specified
- 266 5. Supports the following additional functions:
 - 267 a. C_GetMechanismList ([PKCS11-~~SPECBase~~] 5.5)
 - 268 b. C_GetMechanismInfo ([PKCS11-~~SPECBase~~] 5.5)
- 269 6. Supports the following additional mechanisms:
 - 270 a. None specified
- 271 7. Supports Error Handling ([PKCS11-~~SPECBase~~] 5.1) for any supported object, function or
- 272 mechanism
- 273 8. Optionally supports any clause within [PKCS11-~~SPECBase~~] that is not listed above
- 274 9. Optionally supports extensions outside the scope of this standard (e.g., vendor defined
- 275 extensions, conformance clauses) that do not contradict any PKCS #11 requirements
- 276 ~~9. Optionally supports extensions outside the scope of this standard (e.g., vendor defined~~
- 277 ~~extensions, conformance clauses) that do not contradict any PKCS11 requirements~~

278 **3.43.5 Extended Provider Clause**

279 This profile builds on the ~~baseline provider clause~~PKCS#11 Baseline Provider to add support for

280 mechanism-based usage.

281 **3.4.13.5.1 Implementation Conformance**

282 An implementation is a conforming Extended Provider ~~Clause~~ if it meets the conditions as outlined in the

283 following section.

284 **3.4.23.5.2 Conformance of a ~~PKCS11~~PKCS #11 Extended Provider**

285 An implementation conforms to this specification as Extended Provider if it meets the following conditions:

- 286 1. Supports the conditions required by the ~~PKCS11~~PKCS #11 conformance clauses ([PKCS11-
- 287 SPECBase] Section 6 (PKCS#11 Implementation Conformance)
- 288 2. Supports the conditions required by the ~~PKCS11~~PKCS #11 Baseline Provider clauses section
- 289 3.3.
- 290 3. Supports the following additional data types:
 - 291 a. CK_MECHANISM_TYPE ([PKCS11-~~SPECBase~~] 3.4)
 - 292 b. CK_MECHANISM ([PKCS11-~~SPECBase~~] 3.4)
 - 293
- 294 4. Supports the following additional objects:
 - 295 a. None specified
- 296 5. Supports the following additional functions:
 - 297 a. C_GetMechanismList ([PKCS11-~~SPECBase~~] 5.5)
 - 298 b. C_GetMechanismInfo ([PKCS11-~~SPECBase~~] 5.5)
 - 299 c. C_Login ([PKCS11-~~SPECBase~~] 5.6)
 - 300 d. C_Logout ([PKCS11-~~SPECBase~~] 5.6)
- 301 6. Supports the following additional mechanisms:
 - 302 a. None specified
- 303 7. Supports Error Handling ([PKCS11-~~SPECBase~~] 5.1) for any supported object, function or
- 304 mechanism
- 305 8. Optionally supports any clause within [PKCS11-~~SPECBase~~] that is not listed above
- 306 9. Optionally supports extensions outside the scope of this standard (e.g., vendor defined
- 307 extensions, conformance clauses) that do not contradict any PKCS #11 requirements

308 ~~9. Optionally supports extensions outside the scope of this standard (e.g., vendor defined~~
309 ~~extensions, conformance clauses) that do not contradict any PKCS11 requirements~~

310 **3.5.3.6 Authentication Token Clause**

311 This profile builds on the ~~PKCS11 provider~~PKCS #11 Baseline Provider and ~~consumer conformance~~
312 ~~clauses/or Baseline Consumer profiles~~ to provide for use in the context of an authentication token.

313 **3.5.13.6.1 Implementation Conformance**

314 An implementation is a conforming Authentication Token if it meets the conditions as outlined in the
315 following section.

316 **3.5.23.6.2 Conformance of a Authentication Token**

317 An implementation conforms to this specification as an Authentication Token if it meets the following
318 conditions:

- 319 1. If the implementation is a consumer then it SHALL support the conditions required by the
320 ~~PKCS11~~PKCS #11 Baseline Consumer Clause (Section 3.2)
- 321 2. If the implementation is a provider then it SHALL support the conditions required by the
322 ~~PKCS11~~PKCS #11 Baseline Provider Clause (Section 3.3)
- 323 3. Supports the following objects:
 - 324 a. CKO_PRIVATE_KEY
 - 325 b. CKO_PUBLIC_KEY
- 326 4. Supports the following functions:
 - 327 a. C_Login
 - 328 b. C_Logout
 - 329 c. C_SignInit
 - 330 d. C_Sign and/or C_SignUpdate and C_SignFinal
- 331 5. Supports the following mechanisms:
 - 332 a. None specified
- 333 6. Optionally supports any clause within [PKCS11-~~SPECBase~~] that is not listed above
- 334 7. Optionally supports extensions outside the scope of this standard (e.g., vendor defined
335 extensions, conformance clauses) that do not contradict any ~~PKCS11~~PKCS #11 requirements.

336

337 Appendix A. Acknowledgments

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

340

341 **Participants:**

342

343 Gil Abel, Athena Smartcard Solutions, Inc.

344 Warren Armstrong, QuintessenceLabs

345 Peter Bartok, Venafi, Inc.

346 Anthony Berglas, Cryptsoft

347 Kelley Burgin, National Security Agency

348 Robert Burns, Thales e-Security

349 Wan-Teh Chang, Google Inc.

350 Hai-May Chao, Oracle

351 Janice Cheng, Vormetric, Inc.

352 Sangrae Cho, Electronics and Telecommunications Research Institute (ETRI)

353 Doron Cohen, SafeNet, Inc.

354 Fadi Cotran, Futurex

355 Tony Cox, Cryptsoft

356 Christopher Duane, EMC

357 Chris Dunn, SafeNet, Inc.

358 Valerie Fenwick, Oracle

359 Terry Fletcher, SafeNet, Inc.

360 Susan Gleeson, Oracle

361 Sven Gossel, Charismathics

362 Robert Griffin, EMC

363 Paul Grojean, Individual

364 Peter Gutmann, Individual

365 Dennis E. Hamilton, Individual

366 Thomas Hardjono, M.I.T.

367 Tim Hudson, Cryptsoft

368 Gershon Janssen, Individual

369 Seunghun Jin, Electronics and Telecommunications Research Institute (ETRI)

370 Andrey Jivsov, Symantec Corp.

371 Greg Kazmierczak, Wave Systems Corp.

372 Mark Knight, Thales e-Security

373 Darren Krahn, Google Inc.

374 Alex Krasnov, Infineon Technologies AG

375 Dina Kurktchi-Nimeh, Oracle

376 Mark Lambiase, SecureAuth Corporation

377 Lawrence Lee, GoTrust Technology Inc.
378 John Leiseboer, QuintessenceLabs
379 Hal Lockhart, Oracle
380 Robert Lockhart, Thales e-Security
381 Dale Moberg, Axway Software
382 Darren Moffat, Oracle
383 Valery Osheter, SafeNet, Inc.
384 Sean Parkinson, EMC
385 Rob Philpott, EMC
386 Mark Powers, Oracle
387 Ajai Puri, SafeNet, Inc.
388 Robert Relyea, Red Hat
389 Saikat Saha, Oracle
390 Subhash Sankuratipati, NetApp
391 Johann Schoetz, Infineon Technologies AG
392 Rayees Shamsuddin, Wave Systems Corp.
393 Radhika Siravara, Oracle
394 Brian Smith, Mozilla Corporation
395 David Smith, Venafi, Inc.
396 Ryan Smith, Futurex
397 Jerry Smith, US Department of Defense (DoD)
398 Oscar So, Oracle
399 Michael Stevens, QuintessenceLabs
400 Michael StJohns, Individual
401 Sander Temme, Thales e-Security
402 Kiran Thota, VMware, Inc.
403 Walter-John Turnes, Gemini Security Solutions, Inc.
404 Stef Walter, Red Hat
405 Jeff Webb, Dell
406 Magda Zdunkiewicz, Cryptsoft
407 Chris Zimman, Bloomberg Finance L.P.

408 **Appendix B. Revision History**

409

Revision	Date	Editor	Changes Made
wd01	20-Mar-2013	Tim Hudson	Template provided by OASIS
wd02	3-Apr-2013	Tim Hudson	Initial draft
wd03	18-Sep-2013	Tim Hudson	Updated draft matching current drafts of the specification
wd04	27-Oct-2013	Robert Griffin	Final participant list and other editorial changes for Committee Specification Draft
wd04a	27-Oct-2013	Tim Hudson	Deleted no longer valid comment and corrected unknown section reference.
<u>wd05</u>	<u>25-Feb-2014</u>	<u>Tim Hudson / Robert Griffin</u>	<u>Incorporated changes from v2.40 public review</u>

410