



# PKCS #11 Cryptographic Token Interface Profiles Version 2.40

## Committee Specification 01

16 September 2014

### Specification URIs

#### This version:

<http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/cs01/pkcs11-profiles-v2.40-cs01.doc>  
(Authoritative)  
<http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/cs01/pkcs11-profiles-v2.40-cs01.html>  
<http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/cs01/pkcs11-profiles-v2.40-cs01.pdf>

#### Previous 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>

#### 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](mailto:robert.griffin@rsa.com)), EMC Corporation  
Valerie Fenwick ([valerie.fenwick@oracle.com](mailto:valerie.fenwick@oracle.com)), Oracle

#### Editor:

Tim Hudson ([tjh@cryptsoft.com](mailto: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 standard.

The PKCS #11 Cryptographic Token Interface 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. 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](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 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-Profiles-v2.40]**

*PKCS #11 Cryptographic Token Interface Profiles Version 2.40*. Edited by Tim Hudson. 16 September 2014. OASIS Committee Specification 01. <http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/cs01/pkcs11-profiles-v2.40-cs01.html>. Latest version: <http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/pkcs11-profiles-v2.40.html>.

---

## Notices

Copyright © OASIS Open 2014. 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.....	11
3.5.1	Implementation Conformance.....	11
3.5.2	Conformance of a PKCS #11 Extended Provider.....	11
3.6	Authentication Token Clause.....	11
3.6.1	Implementation Conformance.....	11
3.6.2	Conformance of a Authentication Token.....	11
Appendix A.	Acknowledgments.....	13
Appendix B.	Revision History.....	16

---

# 1 Introduction

## 1.1 Description of this Document

OASIS requires a conformance section in an approved committee specification ([PKCS11-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-Base] Section 6 (PKCS#11 Implementation Conformance) through profiles that define the use of 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 PKCS #11 within a particular environment or context of use. They may, optionally, require the use of specific PKCS #11 functionality or in other respects define the processing rules to be followed by profile actors.

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

## 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].

## 1.3 Normative References

- [PKCS11-Base]** *PKCS #11 Cryptographic Token Interface Base Specification Version 2.40.* Edited by Susan Gleeson and Chris Zimman. 16 September 2014. OASIS Committee Specification 01. <http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/cs01/pkcs11-base-v2.40-cs01.html>. Latest version: <http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/pkcs11-base-v2.40.html>.
- [PKCS11-Curr]** *PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40.* Edited by Susan Gleeson and Chris Zimman. 16 September 2014. OASIS Committee Specification 01. <http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/cs01/pkcs11-curr-v2.40-cs01.html>. Latest version: <http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/pkcs11-curr-v2.40.html>.
- [PKCS11-Hist]** *PKCS #11 Cryptographic Token Interface Historical Mechanisms Specification Version 2.40.* Edited by Susan Gleeson and Chris Zimman. 16 September 2014. OASIS Committee Specification 01. <http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/cs01/pkcs11-hist-v2.40-cs01.html>. Latest version: <http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/pkcs11-hist-v2.40.html>.
- [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>.

46 **1.4 Non-Normative References**

47 **[PKCS11-UG]** *PKCS #11 Cryptographic Token Interface Usage Guide Version 2.40*. Edited by  
48 John Leiseboer and Robert Griffin. 16 September 2014. OASIS Committee Note  
49 01. [http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cn01/pkcs11-ug-v2.40-](http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cn01/pkcs11-ug-v2.40-cn01.html)  
50 [cn01.html](http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/cn01/pkcs11-ug-v2.40-cn01.html). Latest version: [http://docs.oasis-open.org/pkcs11-](http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/pkcs11-ug-v2.40.html)  
51 [ug/v2.40/pkcs11-ug-v2.40.html](http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/pkcs11-ug-v2.40.html).  
52

---

## 53 2 Profiles

### 54 2.1 PKCS #11 Profiles

55 This document defines a selected set of conformance clauses which form PKCS #11 Profiles. The PKCS  
56 11 TC also welcomes proposals for new profiles. PKCS 11 TC members are encouraged to submit these  
57 proposals to the PKCS 11 TC for consideration for inclusion in a future version of this TC-approved  
58 document. However, some OASIS members MAY simply wish to inform the committee of profiles or other  
59 work related to PKCS #11.

### 60 2.2 Guidelines for Specifying Conformance Clauses

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

- 62 1. Implement functionality as mandated by **[PKCS11-Base] Section 6** (PKCS#11 Implementation  
63 Conformance)
- 64 2. Specify the list of additional data types that SHALL be supported
- 65 3. Specify the list of additional objects that SHALL be supported
- 66 4. Specify the list of additional functions that SHALL be supported
- 67 5. Specify the list of additional mechanisms that SHALL be supported

68

### 69 2.3 Guidelines for Validating Conformance to PKCS #11 Profiles

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

- 72 • All data types specified as required in that profile
- 73 • All objects specified as required in that profile
- 74 • All functions specified as required in that profile
- 75 • All mechanisms specified as required in that profile

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

- 78 • All data types specified as required in that profile
- 79 • All objects specified as required in that profile
- 80 • All functions specified as required in that profile
- 81 • All mechanisms specified as required in that profile

82

---

## 83 3 Conformance

### 84 3.1 Purpose of this Section

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

### 87 3.2 Baseline Consumer Clause

88 A PKCS #11 consumer calls a PKCS #11 provider implementation of the PKCS #11 API in order to use  
89 the cryptographic functionality from that provider.

90

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

#### 93 3.2.1 Implementation Conformance

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

#### 96 3.2.2 Conformance of a PKCS #11 Baseline Consumer

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

- 99 1. Supports the conditions required by the PKCS #11 conformance clauses ([PKCS11-Base]  
100 Section 6 (PKCS#11 Implementation Conformance))
- 101 2. Supports the following data types:
  - 102 a. CK\_VERSION ([PKCS11-Base] 3.1)
  - 103 b. CK\_INFO ([PKCS11-Base] 3.1)
  - 104 c. CK\_SLOT\_ID ([PKCS11-Base] 3.2)
  - 105 d. CK\_SLOT\_INFO ([PKCS11-Base] 3.2)
  - 106 e. CK\_TOKEN\_INFO ([PKCS11-Base] 3.2)
  - 107 f. CK\_SESSION\_HANDLE ([PKCS11-Base] 3.3)
  - 108 g. CK\_USER\_TYPE ([PKCS11-Base] 3.3)
  - 109 h. CK\_SESSION\_INFO ([PKCS11-Base] 3.3)
  - 110 i. CK\_OBJECT\_HANDLE ([PKCS11-Base] 3.4)
  - 111 j. CK\_OBJECT\_CLASS ([PKCS11-Base] 3.4)
  - 112 k. CK\_ATTRIBUTE\_TYPE ([PKCS11-Base] 3.4)
  - 113 l. CK\_ATTRIBUTE ([PKCS11-Base] 3.4)
  - 114 m. CK\_RV ([PKCS11-Base] 3.6)
  - 115 n. CK\_FUNCTION\_LIST ([PKCS11-Base] 3.6)
  - 116 o. CK\_C\_INITIALIZE\_ARGS ([PKCS11-Base] 3.7)
- 117 3. Supports the following objects:
  - 118 a. CKA\_CLASS ([PKCS11-Base] 4.2)
  - 119 b. CKA\_VALUE ([PKCS11-Base])
- 120 4. Supports the following functions:
  - 121 a. C\_GetFunctionList ([PKCS11-Base] 5.4)
  - 122 b. C\_Initialize ([PKCS11-Base] 5.4)
  - 123 c. C\_Finalize ([PKCS11-Base] 5.4)
  - 124 d. C\_GetInfo ([PKCS11-Base] 5.4)
  - 125 e. C\_GetSlotList ([PKCS11-Base] 5.5)



- 126 f. C\_GetSlotInfo ([PKCS11-Base] 5.5)
- 127 g. C\_GetTokenInfo ([PKCS11-Base] 5.5)
- 128 h. C\_OpenSession ([PKCS11-Base] 5.6)
- 129 i. C\_CloseSession ([PKCS11-Base] 5.6)
- 130 5. Supports the following mechanisms:
- 131 a. None specified
- 132 6. Supports Error Handling ([PKCS11-Base] 5.1) for any supported object, function or mechanism
- 133 7. Optionally supports any clause within [PKCS11-Base] that is not listed above
- 134 8. Optionally supports extensions outside the scope of this standard (e.g., vendor defined
- 135 extensions, conformance clauses) that do not contradict any PKCS #11 requirements

### 136 3.3 Baseline Provider Clause

137 A PKCS #11 provider makes cryptographic functionality available to a consuming application in terms of  
138 the PKCS #11 API.

139 This profile specifies the most basic functionality that would be expected of a conformant PKCS #11  
140 provider – the ability to provide information about the capabilities of the cryptographic services provided.

#### 141 3.3.1 Implementation Conformance

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

#### 144 3.3.2 Conformance of a PKCS #11 Baseline Provider

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

- 147 1. Supports the conditions required by the PKCS #11 conformance clauses ([PKCS11-Base]  
148 Section 6 (PKCS#11 Implementation Conformance))
- 149 2. Supports the following data types:
  - 150 a. CK\_VERSION ([PKCS11-Base] 3.1)
  - 151 b. CK\_INFO ([PKCS11-Base] 3.1)
  - 152 c. CK\_SLOT\_ID ([PKCS11-Base] 3.2)
  - 153 d. CK\_SLOT\_INFO ([PKCS11-Base] 3.2)
  - 154 e. CK\_TOKEN\_INFO ([PKCS11-Base] 3.2)
  - 155 f. CK\_SESSION\_HANDLE ([PKCS11-Base] 3.3)
  - 156 g. CK\_USER\_TYPE ([PKCS11-Base] 3.3)
  - 157 h. CK\_SESSION\_INFO ([PKCS11-Base] 3.3)
  - 158 i. CK\_OBJECT\_HANDLE ([PKCS11-Base] 3.4)
  - 159 j. CK\_OBJECT\_CLASS ([PKCS11-Base] 3.4)
  - 160 k. CK\_ATTRIBUTE\_TYPE ([PKCS11-Base] 3.4)
  - 161 l. CK\_ATTRIBUTE ([PKCS11-Base] 3.4)
  - 162 m. CK\_RV ([PKCS11-Base] 3.6)
  - 163 n. CK\_FUNCTION\_LIST ([PKCS11-Base] 3.6)
  - 164 o. CK\_C\_INITIALIZE\_ARGS ([PKCS11-Base] 3.7)
- 165 3. Supports the following objects:
  - 166 a. CKA\_CLASS ([PKCS11-Base] 4.2)
  - 167 b. CKA\_TOKEN ([PKCS11-Base] 4.2)
  - 168 c. CKA\_VALUE ([PKCS11-Base])
  - 169 d. CKA\_ID ([PKCS11-Base])
  - 170 e. CKA\_PRIVATE ([PKCS11-Base] x.y)
  - 171 f. CKA\_MODIFIABLE ([PKCS11-Base])
  - 172 g. CKA\_LABEL ([PKCS11-Base])
- 173 4. Supports the following functions:

- 174 a. C\_GetFunctionList ([PKCS11-Base] 5.4)
  - 175 b. C\_Initialize ([PKCS11-Base] 5.4)
  - 176 c. C\_Finalize ([PKCS11-Base] 5.4)
  - 177 d. C\_GetInfo ([PKCS11-Base] 5.4)
  - 178 e. C\_GetSlotList ([PKCS11-Base] 5.5)
  - 179 f. C\_GetSlotInfo ([PKCS11-Base] 5.5)
  - 180 g. C\_GetTokenInfo ([PKCS11-Base] 5.5)
  - 181 h. C\_OpenSession ([PKCS11-Base] 5.6)
  - 182 i. C\_CloseSession ([PKCS11-Base] 5.6)
  - 183 j. C\_GetSessionInfo ([PKCS11-Base] 5.6)
  - 184 k. C\_FindObjectsInit ([PKCS11-Base] 5.6)
  - 185 l. C\_FindObjects ([PKCS11-Base] 5.6)
  - 186 m. C\_FindObjectsFinal ([PKCS11-Base] 5.6)
  - 187 n. C\_GetAttributeValue ([PKCS11-Base] 5.7)
- 188 5. Supports the following mechanisms:
- 189 a. None specified
- 190 6. Supports Error Handling ([PKCS11-Base] 5.1) for any supported object, function or mechanism
- 191 7. Optionally supports any clause within [PKCS11-Base] that is not listed above
- 192 8. Optionally supports extensions outside the scope of this standard (e.g., vendor defined
- 193 extensions, conformance clauses) that do not contradict any PKCS #11 requirements

## 194 3.4 Extended Consumer Clause

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

### 197 3.4.1 Implementation Conformance

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

### 200 3.4.2 Conformance of a PKCS #11 Extended Consumer

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

- 203 1. Supports the conditions required by the PKCS11 conformance clauses ([PKCS11-Base] Section  
204 6 (PKCS#11 Implementation Conformance))
- 205 2. Supports the conditions required by the PKCS11 Baseline Consumer clauses section 3.2
- 206 3. Supports the following additional data types:
  - 207 a. CK\_MECHANISM\_TYPE ([PKCS11-Base] 3.4)
  - 208 b. CK\_MECHANISM ([PKCS11-Base] 3.4)
- 209 4. Supports the following additional objects:
  - 210 a. None specified
- 211 5. Supports the following additional functions:
  - 212 a. C\_GetMechanismList ([PKCS11-Base] 5.5)
  - 213 b. C\_GetMechanismInfo ([PKCS11-Base] 5.5)
- 214 6. Supports the following additional mechanisms:
  - 215 a. None specified
- 216 7. Supports Error Handling ([PKCS11-Base] 5.1) for any supported object, function or mechanism
- 217 8. Optionally supports any clause within [PKCS11-Base] that is not listed above
- 218 9. Optionally supports extensions outside the scope of this standard (e.g., vendor defined  
219 extensions, conformance clauses) that do not contradict any PKCS #11 requirements

## 220 **3.5 Extended Provider Clause**

221 This profile builds on the PKCS#11 Baseline Provider to add support for mechanism-based usage.

### 222 **3.5.1 Implementation Conformance**

223 An implementation is a conforming Extended Provider if it meets the conditions as outlined in the  
224 following section.

### 225 **3.5.2 Conformance of a PKCS #11 Extended Provider**

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

- 227 1. Supports the conditions required by the PKCS #11 conformance clauses ([PKCS11-Base]  
228 Section 6 (PKCS#11 Implementation Conformance)
- 229 2. Supports the conditions required by the PKCS #11 Baseline Provider clauses section 3.3.
- 230 3. Supports the following additional data types:
  - 231 a. CK\_MECHANISM\_TYPE ([PKCS11-Base] 3.4)
  - 232 b. CK\_MECHANISM ([PKCS11-Base] 3.4)
  - 233
- 234 4. Supports the following additional objects:
  - 235 a. None specified
- 236 5. Supports the following additional functions:
  - 237 a. C\_GetMechanismList ([PKCS11-Base] 5.5)
  - 238 b. C\_GetMechanismInfo ([PKCS11-Base] 5.5)
  - 239 c. C\_Login ([PKCS11-Base] 5.6)
  - 240 d. C\_Logout ([PKCS11-Base] 5.6)
- 241 6. Supports the following additional mechanisms:
  - 242 a. None specified
- 243 7. Supports Error Handling ([PKCS11-Base] 5.1) for any supported object, function or mechanism
- 244 8. Optionally supports any clause within [PKCS11-Base] that is not listed above
- 245 9. Optionally supports extensions outside the scope of this standard (e.g., vendor defined  
246 extensions, conformance clauses) that do not contradict any PKCS #11 requirements

## 247 **3.6 Authentication Token Clause**

248 This profile builds on the PKCS #11 Baseline Provider and/or Baseline Consumer profiles to provide for  
249 use in the context of an authentication token.

### 250 **3.6.1 Implementation Conformance**

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

### 253 **3.6.2 Conformance of a Authentication Token**

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

- 256 1. If the implementation is a consumer then it SHALL support the conditions required by the PKCS  
257 #11 Baseline Consumer Clause (Section 3.2)
- 258 2. If the implementation is a provider then it SHALL support the conditions required by the PKCS  
259 #11 Baseline Provider Clause (Section 3.3)
- 260 3. Supports the following objects:

- 261           a. CKO\_PRIVATE\_KEY
- 262           b. CKO\_PUBLIC\_KEY
- 263       4. Supports the following functions:
- 264           a. C\_Login
- 265           b. C\_Logout
- 266           c. C\_SignInit
- 267           d. C\_Sign and/or C\_SignUpdate and C\_SignFinal
- 268       5. Supports the following mechanisms:
- 269           a. None specified
- 270       6. Optionally supports any clause within [PKCS11-Base] that is not listed above
- 271       7. Optionally supports extensions outside the scope of this standard (e.g., vendor defined
- 272           extensions, conformance clauses) that do not contradict any PKCS #11 requirements.
- 273

---

## 274 Appendix A. Acknowledgments

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

277

### 278 **Participants:**

279

280 Gil Abel, Athena Smartcard Solutions, Inc.

281 Warren Armstrong, QuintessenceLabs

282 Jeff Bartell, Semper Foris Solutions LLC

283 Peter Bartok, Venafi, Inc.

284 Anthony Berglas, Cryptsoft

285 Joseph Brand, Semper Fortis Solutions LLC

286 Kelley Burgin, National Security Agency

287 Robert Burns, Thales e-Security

288 Wan-Teh Chang, Google Inc.

289 Hai-May Chao, Oracle

290 Janice Cheng, Vormetric, Inc.

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

292 Doron Cohen, SafeNet, Inc.

293 Fadi Cotran, Futurex

294 Tony Cox, Cryptsoft

295 Christopher Duane, EMC

296 Chris Dunn, SafeNet, Inc.

297 Valerie Fenwick, Oracle

298 Terry Fletcher, SafeNet, Inc.

299 Susan Gleeson, Oracle

300 Sven Gossel, Charismathics

301 John Green, QuintessenceLabs

302 Robert Griffin, EMC

303 Paul Grojean, Individual

304 Peter Gutmann, Individual

305 Dennis E. Hamilton, Individual

306 Thomas Hardjono, M.I.T.

307 Tim Hudson, Cryptsoft

308 Gershon Janssen, Individual

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

310 Wang Jingman, Feitan Technologies

311 Andrey Jivsov, Symantec Corp.

312 Mark Joseph, P6R

313 Stefan Kaesar, Infineon Technologies

314 Greg Kazmierczak, Wave Systems Corp.  
315 Mark Knight, Thales e-Security  
316 Darren Krahn, Google Inc.  
317 Alex Krasnov, Infineon Technologies AG  
318 Dina Kurktchi-Nimeh, Oracle  
319 Mark Lambiase, SecureAuth Corporation  
320 Lawrence Lee, GoTrust Technology Inc.  
321 John Leiseboer, QuintessenceLabs  
322 Sean Leon, Infineon Technologies  
323 Geoffrey Li, Infineon Technologies  
324 Howie Liu, Infineon Technologies  
325 Hal Lockhart, Oracle  
326 Robert Lockhart, Thales e-Security  
327 Dale Moberg, Axway Software  
328 Darren Moffat, Oracle  
329 Valery Osheter, SafeNet, Inc.  
330 Sean Parkinson, EMC  
331 Rob Philpott, EMC  
332 Mark Powers, Oracle  
333 Ajai Puri, SafeNet, Inc.  
334 Robert Relyea, Red Hat  
335 Saikat Saha, Oracle  
336 Subhash Sankuratripati, NetApp  
337 Anthony Scarpino, Oracle  
338 Johann Schoetz, Infineon Technologies AG  
339 Rayees Shamsuddin, Wave Systems Corp.  
340 Radhika Siravara, Oracle  
341 Brian Smith, Mozilla Corporation  
342 David Smith, Venafi, Inc.  
343 Ryan Smith, Futurex  
344 Jerry Smith, US Department of Defense (DoD)  
345 Oscar So, Oracle  
346 Graham Steel, Cryptosense  
347 Michael Stevens, QuintessenceLabs  
348 Michael StJohns, Individual  
349 Jim Susoy, P6R  
350 Sander Temme, Thales e-Security  
351 Kiran Thota, VMware, Inc.  
352 Walter-John Turnes, Gemini Security Solutions, Inc.  
353 Stef Walter, Red Hat  
354 James Wang, Vormetric  
355 Jeff Webb, Dell

356 Peng Yu, Feitian Technologies  
357 Magda Zdunkiewicz, Cryptsoft  
358 Chris Zimman, Individual  
359

360

## Appendix B. Revision History

361

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.
csd01	30-Oct-2013	OASIS	Committee Specification Draft
wd05	25-Feb-2014	Tim Hudson / Robert Griffin	Incorporated changes from v2.40 public review
csd02	23-Apr-2014	OASIS	Committee Specification Draft
csd02a	Sep 3 2013	Robert Griffin	Updated revision history and participant list in preparation for Committee Specification ballot

362

363