



# PKCS #11 Cryptographic Token Interface Historical Mechanisms Specification Version 2.40

Committee Specification Draft 01 /  
Public Review Draft 01

30 October 2013

## Specification URIs

This version:

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

Previous version:

N/A

Latest version:

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

Editors:

Susan Gleeson ([susan.gleeson@oracle.com](mailto:susan.gleeson@oracle.com)), Oracle  
Chris Zimman ([czimman@bloomberg.com](mailto:czimman@bloomberg.com)), Bloomberg Finance L.P.

Related work:

This specification is related to:

- *PKCS #11 Cryptographic Token Interface Base Specification Version 2.40*. 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*. Latest version. <http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/pkcs11-curr-v2.40.html>.
- *PKCS #11 Cryptographic Token Interface Usage Guide Version 2.40*. Latest version. <http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/pkcs11-ug-v2.40.html>.
- *PKCS #11 Cryptographic Token Interface Profiles Version 2.40*. Latest version. <http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/pkcs11-profiles-v2.40.html>.

Abstract:

This document defines mechanisms for PKCS #11 that are no longer in general use.

**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 <http://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 (<http://www.oasis-open.org/committees/pkcs11/ipr.php>).

**Citation format:**

When referencing this specification the following citation format should be used:

**[PKCS11-hist]**

*PKCS #11 Cryptographic Token Interface Historical Mechanisms Specification Version 2.40*. 30 October 2013. OASIS Committee Specification Draft 01 / Public Review Draft 01.  
<http://docs.oasis-open.org/pkcs11/pkcs11-hist/v2.40/csprd01/pkcs11-hist-v2.40-csprd01.html>.

---

## Notices

Copyright © OASIS Open 2013. 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 <http://www.oasis-open.org/policies-guidelines/trademark> for above guidance.

---

# Table of Contents

1	Introduction .....	8
1.1	Terminology .....	8
1.2	Definitions .....	8
1.3	Normative References .....	9
1.4	Non-Normative References .....	9
2	Mechanisms .....	13
2.1	FORTEZZA timestamp .....	16
2.2	KEA .....	16
2.2.1	Definitions .....	16
2.2.2	KEA mechanism parameters .....	16
2.2.3	KEA public key objects .....	17
2.2.4	KEA private key objects .....	18
2.2.5	KEA key pair generation .....	18
2.2.6	KEA key derivation .....	19
2.3	RC2 .....	20
2.3.1	Definitions .....	20
2.3.2	RC2 secret key objects .....	20
2.3.3	RC2 mechanism parameters .....	21
2.3.4	RC2 key generation .....	22
2.3.5	RC2-ECB .....	22
2.3.6	RC2-CBC .....	23
2.3.7	RC2-CBC with PKCS padding .....	23
2.3.8	General-length RC2-MAC .....	24
2.3.9	RC2-MAC .....	24
2.4	RC4 .....	25
2.4.1	Definitions .....	25
2.4.2	RC4 secret key objects .....	25
2.4.3	RC4 key generation .....	25
2.4.4	RC4 mechanism .....	26
2.5	RC5 .....	26
2.5.1	Definitions .....	26
2.5.2	RC5 secret key objects .....	26
2.5.3	RC5 mechanism parameters .....	27
2.5.4	RC5 key generation .....	28
2.5.5	RC5-ECB .....	28
2.5.6	RC5-CBC .....	29
2.5.7	RC5-CBC with PKCS padding .....	29
2.5.8	General-length RC5-MAC .....	30
2.5.9	RC5-MAC .....	30
2.6	General block cipher .....	31
2.6.1	Definitions .....	31
2.6.2	DES secret key objects .....	32
2.6.3	CAST secret key objects .....	33

2.6.4 CAST3 secret key objects .....	33
2.6.5 CAST128 (CAST5) secret key objects .....	34
2.6.6 IDEA secret key objects .....	34
2.6.7 CDMF secret key objects .....	35
2.6.8 General block cipher mechanism parameters.....	35
2.6.9 General block cipher key generation.....	35
2.6.10 General block cipher ECB .....	36
2.6.11 General block cipher CBC.....	36
2.6.12 General block cipher CBC with PKCS padding.....	37
2.6.13 General-length general block cipher MAC .....	38
2.6.14 General block cipher MAC .....	38
2.7 SKIPJACK.....	39
2.7.1 Definitions.....	39
2.7.2 SKIPJACK secret key objects .....	39
2.7.3 SKIPJACK Mechanism parameters .....	40
2.7.4 SKIPJACK key generation .....	42
2.7.5 SKIPJACK-ECB64 .....	42
2.7.6 SKIPJACK-CBC64 .....	42
2.7.7 SKIPJACK-OFB64 .....	42
2.7.8 SKIPJACK-CFB64.....	43
2.7.9 SKIPJACK-CFB32.....	43
2.7.10 SKIPJACK-CFB16.....	43
2.7.11 SKIPJACK-CFB8.....	44
2.7.12 SKIPJACK-WRAP .....	44
2.7.13 SKIPJACK-PRIVATE-WRAP .....	44
2.7.14 SKIPJACK-RELAYX.....	44
2.8 BATON.....	44
2.8.1 Definitions.....	44
2.8.2 BATON secret key objects .....	45
2.8.3 BATON key generation .....	45
2.8.4 BATON-ECB128 .....	46
2.8.5 BATON-ECB96.....	46
2.8.6 BATON-CBC128 .....	46
2.8.7 BATON-COUNTER .....	47
2.8.8 BATON-SHUFFLE .....	47
2.8.9 BATON WRAP .....	47
2.9 JUNIPER.....	47
2.9.1 Definitions.....	47
2.9.2 JUNIPER secret key objects .....	48
2.9.3 JUNIPER key generation .....	48
2.9.4 JUNIPER-ECB128 .....	49
2.9.5 JUNIPER-CBC128 .....	49
2.9.6 JUNIPER-COUNTER .....	49
2.9.7 JUNIPER-SHUFFLE .....	49
2.9.8 JUNIPER WRAP .....	50

2.10 MD2 .....	50
2.10.1 Definitions .....	50
2.10.2 MD2 digest .....	50
2.10.3 General-length MD2-HMAC .....	50
2.10.4 MD2-HMAC .....	51
2.10.5 MD2 key derivation .....	51
2.11 MD5 .....	51
2.11.1 Definitions .....	51
2.11.2 MD5 Digest .....	52
2.11.3 General-length MD5-HMAC .....	52
2.11.4 MD5-HMAC .....	52
2.11.5 MD5 key derivation .....	52
2.12 FASTHASH .....	53
2.12.1 Definitions .....	53
2.12.2 FASTHASH digest .....	53
2.13 PKCS #5 and PKCS #5-style password-based encryption (PBD) .....	53
2.13.1 Definitions .....	53
2.13.2 Password-based encryption/authentication mechanism parameters .....	54
2.13.3 MD2-PBE for DES-CBC .....	54
2.13.4 MD5-PBE for DES-CBC .....	54
2.13.5 MD5-PBE for CAST-CBC .....	55
2.13.6 MD5-PBE for CAST3-CBC .....	55
2.13.7 MD5-PBE for CAST128-CBC (CAST5-CBC) .....	55
2.13.8 SHA-1-PBE for CAST128-CBC (CAST5-CBC) .....	55
2.14 PKCS #12 password-based encryption/authentication mechanisms .....	56
2.14.1 SHA-1-PBE for 128-bit RC4 .....	56
2.14.2 SHA-1_PBE for 40-bit RC4 .....	57
2.14.3 SHA-1_PBE for 128-bit RC2-CBC .....	57
2.14.4 SHA-1_PBE for 40-bit RC2-CBC .....	57
2.15 RIPE-MD .....	57
2.15.1 Definitions .....	57
2.15.2 RIPE-MD 128 Digest .....	58
2.15.3 General-length RIPE-MD 128-HMAC .....	58
2.15.4 RIPE-MD 128-HMAC .....	58
2.15.5 RIPE-MD 160 .....	58
2.15.6 General-length RIPE-MD 160-HMAC .....	58
2.15.7 RIPE-MD 160-HMAC .....	59
2.16 SET .....	59
2.16.1 Definitions .....	59
2.16.2 SET mechanism parameters .....	59
2.16.3 OAEP key wrapping for SET .....	59
2.17 LYNKS .....	60
2.17.1 Definitions .....	60
2.17.2 LYNKS key wrapping .....	60
3 PKCS #11 Implementation Conformance .....	61

Appendix A. Acknowledgments ..... 62  
Appendix B. Manifest constants ..... 64  
Appendix C. Revision History ..... 67

---

# 1 Introduction

This document defines historical PKCS#11 mechanisms, that is, mechanisms that were defined for earlier versions of PKCS #11 but are no longer in general use

All text is normative unless otherwise labeled.

## 1.1 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 **[PKCS #11-Base]** *PKCS #11 Cryptographic Token Interface Base Specification Version 2.40*. Latest version. <http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/pkcs11-base-v2.40.html>.

**[PKCS #11-Curr]** *PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40*. Latest version. <http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/pkcs11-curr-v2.40.html>.

**[PKCS #11-Prof]** *PKCS #11 Cryptographic Token Interface Profiles Version 2.40*. Latest version. <http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/pkcs11-profiles-v2.40.html>.

**[RFC2119]**.

## 1.2 Definitions

For the purposes of this standard, the following definitions apply. Please refer to [PKCS#11-Base] for further definitions

<b>BATON</b>	MISSI's BATON block cipher.
<b>CAST</b>	Entrust Technologies' proprietary symmetric block cipher
<b>CAST3</b>	Entrust Technologies' proprietary symmetric block cipher
<b>CAST5</b>	Another name for Entrust Technologies' symmetric block cipher CAST128. CAST128 is the preferred name.
<b>CAST128</b>	Entrust Technologies' symmetric block cipher.
<b>CDMF</b>	Commercial Data Masking Facility, a block encipherment method specified by International Business Machines Corporation and based on DES.
<b>CMS</b>	Cryptographic Message Syntax (see RFC 2630)
<b>DES</b>	Data Encryption Standard, as defined in FIPS PUB 46-3
<b>ECB</b>	Electronic Codebook mode, as defined in FIPS PUB 81.
<b>FASTHASH</b>	MISSI's FASTHASH message-digesting algorithm.
<b>IDEA</b>	Ascom Systec's symmetric block cipher.
<b>IV</b>	Initialization Vector.
<b>JUNIPER</b>	MISSI's JUNIPER block cipher.
<b>KEA</b>	MISSI's Key Exchange Algorithm.
<b>LYNKS</b>	A smart card manufactured by SPYRUS.



41	<b>MAC</b>	Message Authentication Code
42	<b>MD2</b>	RSA Security's MD2 message-digest algorithm, as defined in RFC
43		1319.
44	<b>MD5</b>	RSA Security's MD5 message-digest algorithm, as defined in RFC
45		1321.
46	<b>PRF</b>	Pseudo random function.
47	<b>RSA</b>	The RSA public-key cryptosystem.
48	<b>RC2</b>	RSA Security's RC2 symmetric block cipher.
49	<b>RC4</b>	RSA Security's proprietary RC4 symmetric stream cipher.
50	<b>RC5</b>	RSA Security's RC5 symmetric block cipher.
51	<b>SET</b>	<b>The Secure Electronic Transaction protocol.</b>
52	<b>SHA-1</b>	The (revised) Secure Hash Algorithm with a 160-bit message digest,
53		as defined in FIPS PUB 180-2.
54	<b>SKIPJACK</b>	MISSI's SKIPJACK block cipher.
55	<b>UTF-8</b>	Universal Character Set (UCS) transformation format (UTF) that
56		represents ISO 10646 and UNICODE strings with a variable number
57		of octets

### 58 1.3 Normative References

59	<b>[PKCS #11-Base]</b>	<i>PKCS #11 Cryptographic Token Interface Base Specification Version 2.40.</i> Latest
60		version. <a href="http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/pkcs11-base-v2.40.html">http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/pkcs11-base-</a>
61		<a href="http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/pkcs11-base-v2.40.html">v2.40.html</a> .
62	<b>[PKCS #11-Curr]</b>	<i>PKCS #11 Cryptographic Token Interface Current Mechanisms Specification</i>
63		<i>Version 2.40.</i> Latest version. <a href="http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/pkcs11-curr-v2.40.html">http://docs.oasis-open.org/pkcs11/pkcs11-</a>
64		<a href="http://docs.oasis-open.org/pkcs11/pkcs11-curr/v2.40/pkcs11-curr-v2.40.html">curr/v2.40/pkcs11-curr-v2.40.html</a> .
65	<b>[PKCS #11-Prof]</b>	<i>PKCS #11 Cryptographic Token Interface Profiles Version 2.40.</i> Latest version.
66		<a href="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-</a>
67		<a href="http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/pkcs11-profiles-v2.40.html">v2.40.html</a> .
68	<b>[RFC2119]</b>	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP
69		14, RFC 2119, March 1997. <a href="http://www.ietf.org/rfc/rfc2119.txt">http://www.ietf.org/rfc/rfc2119.txt</a> .

### 70 1.4 Non-Normative References

71	<b>[ANSI C]</b>	ANSI/ISO. <i>American National Standard for Programming Languages – C.</i> 1990
72	<b>[ANSI X9.31]</b>	Accredited Standards Committee X9. <i>Digital Signatures Using Reversible Public</i>
73		<i>Key Cryptography for the Financial Services Industry (rDSA).</i> 1998.
74	<b>[ANSI X9.42]</b>	Accredited Standards Committee X9. <i>Public Key Cryptography for the Financial</i>
75		<i>Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm</i>
76		<i>Cryptography.</i> 2003
77	<b>[ANSI X9.62]</b>	Accredited Standards Committee X9. <i>Public Key Cryptography for the Financial</i>
78		<i>Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).</i> 1998
79	<b>[CC/PP]</b>	W3C. <i>Composite Capability/Preference Profiles (CC/PP): Structure and</i>
80		<i>Vocabularies.</i> World Wide Web Consortium, January 2004. URL:
81		<a href="http://www.w3.org/RT/CCPP-struct-vocab/">http://www.w3.org/RT/CCPP-struct-vocab/</a>
82	<b>[CDPD]</b>	Ameritech Mobile Communications et al. <i>Cellular Digital Packet Data System</i>
83		<i>Specifications: Part 406: Airlink Security.</i> 1993
84	<b>[FIPS PUB 46-3]</b>	NIST. <i>FIPS 46-3: Data Encryption Standard (DES).</i> October 26, 2999. URL:
85		<a href="http://csrc.nist.gov/publications/fips/index.html">http://csrc.nist.gov/publications/fips/index.html</a>

- 86 [FIPS PUB 74] NIST. *FIPS 74: Guidelines for Implementing and Using the NBS Data Encryption*  
87 *Standard*. April 1, 1981. URL: <http://csrc.nist.gov/publications/fips/index.html>
- 88 [FIPS PUB 81] NIST. *FIPS 81: DES Modes of Operation*. December 1980. URL:  
89 <http://csrc.nist.gov/publications/fips/index.html>
- 90 [FIPS PUB 113] NIST. *FIPS 113: Computer Data Authentication*. May 30, 1985. URL:  
91 <http://csrc.nist.gov/publications/fips/index.html>
- 92 [FIPS PUB 180-2] NIST. *FIPS 180-2: Secure Hash Standard*. August 1, 2002. URL:  
93 <http://csrc.nist.gov/publications/fips/index.html>
- 94 [FIPS PUB 186-2] NIST. *FIPS 186-2: Digital Signature Standard*. January 27, 2000. URL:  
95 <http://csrc.nist.gov/publications/fips/index.html>
- 96 [FIPS PUB 197] NIST. *FIPS 197: Advanced Encryption Standard (AES)*. November 26, 2001.  
97 URL: <http://csrc.nist.gov/publications/fips/index.html>
- 98 [FORTEZZA CIPG] NSA, Workstation Security Products. *FORTEZZA Cryptologic Interface*  
99 *Programmers Guide, Revision 1.52*. November 1985
- 100 [GCS-API] X/Open Company Ltd. *Generic Cryptographic Service API (GCS-API), Base –*  
101 *Draft 2*. February 14, 1995.
- 102 [ISO/IEC 7816-1] ISO. *Information Technology – Identification Cards – Integrated Circuit(s) with*  
103 *Contacts – Part 1: Physical Characteristics*. 1998.
- 104 [ISO/IEC 7816-4] ISO. *Information Technology – Identification Cards – Integrated Circuit(s) with*  
105 *Contacts – Part 4: Interindustry Commands for Interchange*. 1995.
- 106 [ISO/IEC 8824-1] ISO. *Information Technology – Abstract Syntax Notation One (ASN.1):*  
107 *Specification of Base Notation*. 2002.
- 108 [ISO/IEC 8825-1] ISO. *Information Technology – ASN.1 Encoding Rules: Specification of Basic*  
109 *Encoding Rules (BER), Canonical Encoding Rules (CER), and Distinguished*  
110 *Encoding Rules (DER)*. 2002.
- 111 [ISO/IEC 9594-1] ISO. *Information Technology – Open System Interconnection – The Directory:*  
112 *Overview of Concepts, Models and Services*. 2001.
- 113 [ISO/IEC 9594-8] ISO. *Information Technology – Open Systems Interconnection – The Directory:*  
114 *Public-key and Attribute Certificate Frameworks*. 2001.
- 115 [ISO/IEC 9796-2] ISO. *Information Technology – Security Techniques – Digital Signature Scheme*  
116 *Giving Message Recovery – Part 2: Integer factorization based mechanisms*.  
117 2002.
- 118 [Java MIDP] Java Community Process. *Mobile Information Device Profile for Java 2 Micro*  
119 *Edition*. November 2002. URL: <http://jcp.org/jsr/detail/118.jsp>
- 120 [MeT-PTD] MeT. *MeT PTD Definition – Personal Trusted Device Definition, Version 1.0*.  
121 February 2003. URL: <http://www.mobiletransaction.org>
- 122 [PCMCIA] Personal Computer Memory Card International Association. *PC Card Standard,*  
123 *Release 2.1*. July 1993.
- 124 [PKCS #1] RSA Laboratories. *RSA Cryptography Standard, v2.1*. June 14, 2002
- 125 [PKCS #3] RSA Laboratories. *Diffie-Hellman Key-Agreement Standard, v1.4*. November  
126 1993.
- 127 [PKCS #5] RSA Laboratories. *Password-Based Encryption Standard, v2.0*. March 26,  
128 1999.
- 129 [PKCS #7] RSA Laboratories. *Cryptographic Message Syntax Standard, v1.5*. November  
130 1993
- 131 [PKCS #8] RSA Laboratories. *Private-Key Information Syntax Standard, v1.2*. November  
132 1993.
- 133 [PKCS #11-UG] *PKCS #11 Cryptographic Token Interface Usage Guide Version 2.40*. Latest  
134 version. [http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/pkcs11-ug-](http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/pkcs11-ug-v2.40.html)  
135 [v2.40.html](http://docs.oasis-open.org/pkcs11/pkcs11-ug/v2.40/pkcs11-ug-v2.40.html).
- 136 [PKCS #11-C] RSA Laboratories. *PKCS#11: Conformance Profile Specification*. October  
137 2000.
- 138 [PKCS #11-P] RSA Laboratories. *PKCS #11 Profiles for mobile devices*. June 2003.

139

140 **[PKCS #12]** RSA Laboratories. *Personal Information Exchange Syntax Standard, v1.0.*  
141 June 1999.

142 **[RFC 1319]** B. Kaliski. *RFC 1319: The MD2 Message-Digest Algorithm.* RSA Laboratories,  
143 April 1992. URL: <http://ietf.org/rfc/rfc1319.txt>

144 **[RFC 1321]** R. Rivest. *RFC 1321: The MD5 Message-Digest Algorithm.* MIT Laboratory for  
145 Computer Science and RSA Data Security, Inc., April 1992. URL:  
146 <http://ietf.org/rfc/rfc1321.txt>

147 **[RFC 1421]** J. Linn. *RFC 1421: Privacy Enhancement for Internet Electronic Mail: Part I:  
148 Message Encryption and Authentication Procedures.* IAB IRTF PSRG, IETF  
149 PEM WG, February 1993. URL: <http://ietf.org/rfc/rfc1421.txt>

150 **[RFC 2045]** Freed, N., and Borenstein. *RFC 2045: Multipurpose Internet Mail Extensions  
151 (MIME) Part One: Format of Internet Message Bodies.* November 1996. URL:  
152 <http://ietf.org/rfc/rfc2045.txt>

153 **[RFC 2246]** T. Dierks and C. Allen. *RFC 2245: The TLS Protocol Version 1.0.* Certicom,  
154 January 1999. URL: <http://ietf.org/rfc/rfc2246.txt>

155 **[RFC 2279]** F. Yergeau. *RFC 2279: UTF-8, a transformation format of ISO 10646.* Alis  
156 Technologies, January 1998. URL: <http://ietf.org/rfc/rfc2279.txt>

157 **[RFC 2534]** Masinter, L., Wing, D., Mutz, A., and K. Holtman. *RFC 2534: Media Features for  
158 Display, Print and Fax.* March 1999. URL: <http://ietf.org/rfc/rfc2534.txt>

159 **[RFC 2630]** R. Houseley. *RFC 2630: cryptographic Message Syntax.* June 1999. URL:  
160 <http://ietf.org/rfc/rfc2630.txt>

161 **[RFC 2743]** J. Linn. *RFC 2743: Generic Security Service Application Program Interface  
162 Version 2, Update 1.* RSA Laboratories, January 2000. URL:  
163 <http://ietf.org/rfc/rfc2743.txt>

164 **[RFC 2744]** J. Wray. *RFC 2744: Generic Security Services API Version 2: C-bindings.* Iris  
165 Associates, January 2000. URL: <http://ietf.org/rfc/rfc2744.txt>

166 **[SEC-1]** Standards for Efficient Cryptography Group (SECG). *Standards for Efficient  
167 Cryptography (SEC) 1: Elliptic Curve Cryptography.* Version 1.0, September 20,  
168 2000.

169 **[SEC-2]** Standards for Efficient cryptography Group (SECG). *Standards for Efficient  
170 Cryptography (SEC) 2: Recommended Elliptic Curve Domain Parameters.*  
171 Version 1.0, September 20, 2000.

172 **[TLS]** IETF. *RFC 2246: The TLS Protocol Version 1.0.* January 1999. URL:  
173 <http://ietf.org/rfc/rfc2256.txt>

174 **[WIM]** WAP. *Wireless Identity Module. – WAP-260-WIP-20010712.a.* July 2001. URL:  
175 <http://www.wapforum.org>

176 **[WPKI]** WAP. *Wireless PKI. – WAP-217-WPKI-20010424-a.* April 2001. URL:  
177 <http://www.wapforum.org>

178 **[WTLS]** WAP. *Wireless Transport Layer Security Version – WAP-261-WTLS-20010406-  
179 a.* April 2001. URL: <http://www.wapforum.org>

180 **[X.500]** ITU-T. *Information Technology – Open Systems Interconnection – The Directory:  
181 Overview of Concepts, Models and Services.* February 2001. (Identical to  
182 ISO/IEC 9594-1)

183 **[X.509]** ITU-T. *Information Technology – Open Systems Interconnection – The  
184 Directory: Public-key and Attribute Certificate Frameworks.* March 2000.  
185 (Identical to ISO/IEC 9594-8)

186 **[X.680]** ITU-T. *Information Technology – Abstract Syntax Notation One (ASN.1):  
187 Specification of Basic Notation.* July 2002. (Identical to ISO/IEC 8824-1)

188 **[X.690]** ITU-T. *Information Technology – ASN.1 Encoding Rules: Specification of Basic  
189 Encoding Rules (BER), Canonical Encoding Rules (CER), and Distinguished  
190 Encoding Rules (DER).* July 2002. (Identical to ISO/IEC 8825-1)

191



193 **2 Mechanisms**

194 A mechanism specifies precisely how a certain cryptographic process is to be performed. PKCS #11  
 195 implementations MAY use one or more mechanisms defined in this document.

196  
 197 The following table shows which Cryptoki mechanisms are supported by different cryptographic  
 198 operations. For any particular token, of course, a particular operation may well support only a subset of  
 199 the mechanisms listed. There is also no guarantee that a token which supports one mechanism for some  
 200 operation supports any other mechanism for any other operation (or even supports that same mechanism  
 201 for any other operation). For example, even if a token is able to create RSA digital signatures with the  
 202 **CKM\_RSA\_PKCS** mechanism, it may or may not be the case that the same token can also perform RSA  
 203 encryption with **CKM\_RSA\_PKCS**.

204 *Table 1, Mechanisms vs. Functions*

Mechanism	Functions						
	Encrypt & Decrypt	Sign & Verify	SR & VR <sup>1</sup>	Digest	Gen. Key/Key Pair	Wrap & Unwrap	Derive
CKM_FORTEZZA_TIMESTAMP		X <sup>2</sup>					
CKM_KEA_KEY_PAIR_GEN					X		
CKM_KEA_KEY_DERIVE							X
CKM_RC2_KEY_GEN					X		
CKM_RC2_ECB	X					X	
CKM_RC2_CBC	X					X	
CKM_RC2_CBC_PAD	X					X	
CKM_RC2_MAC_GENERAL		X					
CKM_RC2_MAC		X					
CKM_RC4_KEY_GEN					X		
CKM_RC4	X						
CKM_RC5_KEY_GEN					X		
CKM_RC5_ECB	X					X	
CKM_RC5_CBC	X					X	
CKM_RC5_CBC_PAD	X					X	
CKM_RC5_MAC_GENERAL		X					
CKM_RC5_MAC		X					
CKM_DES_KEY_GEN					X		
CKM_DES_ECB	X					X	
CKM_DES_CBC	X					X	
CKM_DES_CBC_PAD	X					X	
CKM_DES_MAC_GENERAL		X					
CKM_DES_MAC		X					
CKM_CAST_KEY_GEN					X		
CKM_CAST_ECB	X					X	
CKM_CAST_CBC	X					X	
CKM_CAST_CBC_PAD	X					X	
CKM_CAST_MAC_GENERAL		X					
CKM_CAST_MAC		X					
CKM_CAST3_KEY_GEN					X		

Mechanism	Functions						
	Encrypt & Decrypt	Sign & Verify	SR & VR <sup>1</sup>	Digest	Gen. Key/ Key Pair	Wrap & Unwrap	Derive
CKM_CAST3_ECB	X					X	
CKM_CAST3_CBC	X					X	
CKM_CAST3_CBC_PAD	X					X	
CKM_CAST3_MAC_GENERAL		X					
CKM_CAST3_MAC		X					
CKM_CAST128_KEY_GEN (CKM_CAST5_KEY_GEN)					X		
CKM_CAST128_ECB (CKM_CAST5_ECB)	X					X	
CKM_CAST128_CBC (CKM_CAST5_CBC)	X					X	
CKM_CAST128_CBC_PAD (CKM_CAST5_CBC_PAD)	X					X	
CKM_CAST128_MAC_GENERAL (CKM_CAST5_MAC_GENERAL)		X					
CKM_CAST128_MAC (CKM_CAST5_MAC)		X					
CKM_IDEA_KEY_GEN					X		
CKM_IDEA_ECB	X					X	
CKM_IDEA_CBC	X					X	
CKM_IDEA_CBC_PAD	X					X	
CKM_IDEA_MAC_GENERAL		X					
CKM_IDEA_MAC		X					
CKM_CDMF_KEY_GEN					X		
CKM_CDMF_ECB	X					X	
CKM_CDMF_CBC	X					X	
CKM_CDMF_CBC_PAD	X					X	
CKM_CDMF_MAC_GENERAL		X					
CKM_CDMF_MAC		X					
CKM_SKIPJACK_KEY_GEN					X		
CKM_SKIPJACK_ECB64	X						
CKM_SKIPJACK_CBC64	X						
CKM_SKIPJACK_OFB64	X						
CKM_SKIPJACK_CFB64	X						
CKM_SKIPJACK_CFB32	X						
CKM_SKIPJACK_CFB16	X						
CKM_SKIPJACK_CFB8	X						
CKM_SKIPJACK_WRAP						X	
CKM_SKIPJACK_PRIVATE_WRAP						X	
CKM_SKIPJACK_RELAYX						X <sup>3</sup>	
CKM_BATON_KEY_GEN					X		
CKM_BATON_ECB128	X						
CKM_BATON_ECB96	X						
CKM_BATON_CBC128	X						
CKM_BATON_COUNTER	X						
CKM_BATON_SHUFFLE	X						

Mechanism	Functions						
	Encrypt & Decrypt	Sign & Verify	SR & VR <sup>1</sup>	Digest	Gen. Key/ Key Pair	Wrap & Unwrap	Derive
CKM_BATON_WRAP						X	
CKM_JUNIPER_KEY_GEN					X		
CKM_JUNIPER_ECB128	X						
CKM_JUNIPER_CBC128	X						
CKM_JUNIPER_COUNTER	X						
CKM_JUNIPER_SHUFFLE	X						
CKM_JUNIPER_WRAP						X	
CKM_MD2				X			
CKM_MD2_HMAC_GENERAL		X					
CKM_MD2_HMAC		X					
CKM_MD2_KEY_DERIVATION							X
CKM_MD5				X			
CKM_MD5_HMAC_GENERAL		X					
CKM_MD5_HMAC		X					
CKM_MD5_KEY_DERIVATION							X
CKM_RIPEMD128				X			
CKM_RIPEMD128_HMAC_GENERAL		X					
CKM_RIPEMD128_HMAC		X					
CKM_RIPEMD160				X			
CKM_RIPEMD160_HMAC_GENERAL		X					
CKM_RIPEMD160_HMAC		X					
CKM_FASTHASH				X			
CKM_PBE_MD2_DES_CBC					X		
CKM_PBE_MD5_DES_CBC					X		
CKM_PBE_MD5_CAST_CBC					X		
CKM_PBE_MD5_CAST3_CBC					X		
CKM_PBE_MD5_CAST128_CBC (CKM_PBE_MD5_CAST5_CBC)					X		
CKM_PBE_SHA1_CAST128_CBC (CKM_PBE_SHA1_CAST5_CBC)					X		
CKM_PBE_SHA1_RC4_128					X		
CKM_PBE_SHA1_RC4_40					X		
CKM_PBE_SHA1_RC2_128_CBC					X		
CKM_PBE_SHA1_RC2_40_CBC					X		
CKM_PBA_SHA1_WITH_SHA1_HMAC					X		
CKM_PKCS5_PBKD2					X		
CKM_KEY_WRAP_SET_OAEP						X	
CKM_KEY_WRAP_LYNKS						X	

205 <sup>1</sup> SR = SignRecover, VR = VerifyRecover.

206 <sup>2</sup> Single-part operations only.

207 <sup>3</sup> Mechanism can only be used for wrapping, not unwrapping.

208 The remainder of this section will present in detail the mechanisms supported by Cryptoki and the  
209 parameters which are supplied to them.

210 In general, if a mechanism makes no mention of the *ulMinKeyLen* and *ulMaxKeyLen* fields of the  
211 CK\_MECHANISM\_INFO structure, then those fields have no meaning for that particular mechanism.  
212

## 213 2.1 FORTEZZA timestamp

214 The FORTEZZA timestamp mechanism, denoted **CKM\_FORTEZZA\_TIMESTAMP**, is a mechanism for  
215 single-part signatures and verification. The signatures it produces and verifies are DSA digital signatures  
216 over the provided hash value and the current time.

217 **It has no parameters.**

218 Constraints on key types and the length of data are summarized in the following table. The input and  
219 output data may begin at the same location in memory.

220 *Table 2, FORTEZZA Timestamp: Key and Data Length*

Function	Key type	Input Length	Output Length
C_Sign <sup>1</sup>	DSA private key	20	40
C_Verify <sup>1</sup>	DSA public key	20,40 <sup>2</sup>	N/A

221 <sup>1</sup> Single-part operations only

222 <sup>2</sup> Data length, signature length

223 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
224 specify the supported range of DSA prime sizes, in bits.

## 225 2.2 KEA

### 226 2.2.1 Definitions

227 This section defines the key type “CKK\_KEA” for type CK\_KEY\_TYPE as used in the CKA\_KEY\_TYPE  
228 attribute of key objects.

229 Mechanisms:

230 CKM\_KEA\_KEY\_PAIR\_GEN

231 CKM\_KEA\_KEY\_DERIVE

### 232 2.2.2 KEA mechanism parameters

#### 233 2.2.2.1 CK\_KEA\_DERIVE\_PARAMS; CK\_KEA\_DERIVE\_PARAMS\_PTR

234

235 **CK\_KEA\_DERIVE\_PARAMS** is a structure that provides the parameters to the **CKM\_KEA\_DERIVE**  
236 mechanism. It is defined as follows:

```
237 typedef struct CK_KEA_DERIVE_PARAMS {  
238     CK_BBOOL isSender;  
239     CK_ULONG ulRandomLen;  
240     CK_BYTE_PTR pRandomA;  
241     CK_BYTE_PTR pRandomB;  
242     CK_ULONG ulPublicDataLen;  
243     CK_BYTE_PTR pPublicData;  
244 } CK_KEA_DERIVE_PARAMS;
```

245

246 The fields of the structure have the following meanings:



247 *isSender* Option for generating the key (called a TEK). The value  
 248 is CK\_TRUE if the sender (originator) generates the  
 249 TEK, CK\_FALSE if the recipient is regenerating the TEK

250 *ulRandomLen* the size of random Ra and Rb in bytes

251 *pRandomA* pointer to Ra data

252 *pRandomB* pointer to Rb data

253 *ulPublicDataLen* other party's KEA public key size

254 *pPublicData* pointer to other party's KEA public key value

255 **CK\_KEA\_DERIVE\_PARAMS\_PTR** is a pointer to a **CK\_KEA\_DERIVE\_PARAMS**.

### 256 2.2.3 KEA public key objects

257 KEA public key objects (object class **CKO\_PUBLIC\_KEY**, key type **CKK\_KEA**) hold KEA public keys.  
 258 The following table defines the KEA public key object attributes, in addition to the common attributes  
 259 defined for this object class:

260 *Table 3, KEA Public Key Object Attributes*

Attribute	Data type	Meaning
CKA_PRIME <sup>1,3</sup>	Big integer	Prime $p$ (512 to 1024 bits, in steps of 64 bits)
CKA_SUBPRIME <sup>1,3</sup>	Big integer	Subprime $q$ (160 bits)
CKA_BASE <sup>1,3</sup>	Big integer	Base $g$ (512 to 1024 bits, in steps of 64 bits)
CKA_VALUE <sup>1,4</sup>	Big integer	Public value $y$

261 <sup>1</sup> Refer to [PKCS #11-Base] table 15 for footnotes

262 The **CKA\_PRIME**, **CKA\_SUBPRIME** and **CKA\_BASE** attribute values are collectively the "KEA domain  
 263 parameters".

264 The following is a sample template for creating a KEA public key object:

```

265 CK_OBJECT_CLASS class = CKO_PUBLIC_KEY;
266 CK_KEY_TYPE keyType = CKK_KEA;
267 CK_UTF8CHAR label[] = "A KEA public key object";
268 CK_BYTE prime[] = {...};
269 CK_BYTE subprime[] = {...};
270 CK_BYTE base[] = {...};
271 CK_BYTE value[] = {...};
272 CK_ATTRIBUTE template[] = {
273     {CKA_CLASS, &class, sizeof(class)},
274     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},
275     {CKA_TOKEN, &>true, sizeof(true)},
276     {CKA_LABEL, label, sizeof(label)-1},
277     {CKA_PRIME, prime, sizeof(prime)},
278     {CKA_SUBPRIME, subprime, sizeof(subprime)},
279     {CKA_BASE, base, sizeof(base)},
280     {CKA_VALUE, value, sizeof(value)}
281 };
  
```

282

## 283 2.2.4 KEA private key objects

284 KEA private key objects (object class **CKO\_PRIVATE\_KEY**, key type **CKK\_KEA**) hold KEA private keys.  
285 The following table defines the KEA private key object attributes, in addition to the common attributes  
286 defined for this object class:

287 *Table 4, KEA Private Key Object Attributes*

Attribute	Data type	Meaning
CKA_PRIME <sup>1,4,6</sup>	Big integer	Prime $p$ (512 to 1024 bits, in steps of 64 bits)
CKA_SUBPRIME <sup>1,4,6</sup>	Big integer	Subprime $q$ (160 bits)
CKA_BASE <sup>1,4,6</sup>	Big integer	Base $g$ (512 to 1024 bits, in steps of 64 bits)
CKA_VALUE <sup>1,4,6,7</sup>	Big integer	Private value $x$

288 Refer to [PKCS #11-Base] table 15 for footnotes

289  
290 The **CKA\_PRIME**, **CKA\_SUBPRIME** and **CKA\_BASE** attribute values are collectively the “KEA domain  
291 parameters”.

292 Note that when generating a KEA private key, the KEA parameters are *not* specified in the key’s  
293 template. This is because KEA private keys are only generated as part of a KEA key *pair*, and the KEA  
294 parameters for the pair are specified in the template for the KEA public key.

295 The following is a sample template for creating a KEA private key object:

```
296 CK_OBJECT_CLASS class = CKO_PRIVATE_KEY;  
297 CK_KEY_TYPE keyType = CKK_KEA;  
298 CK_UTF8CHAR label[] = "A KEA private key object";  
299 CK_BYTE subject[] = {...};  
300 CK_BYTE id[] = {123};  
301 CK_BYTE prime[] = {...};  
302 CK_BYTE subprime[] = {...};  
303 CK_BYTE base[] = {...};  
304 CK_BYTE value[] = {...};  
305 CK_BBOOL true = CK_TRUE;  
306 CK_ATTRIBUTE template[] = {  
307     {CKA_CLASS, &class, sizeof(class)},  
308     {CKA_KEY_TYPE, &keyType, sizeof(keyType)}, Algorithm, as defined by NISTS  
309     {CKA_TOKEN, &>true, sizeof(true)},  
310     {CKA_LABEL, label, sizeof(label) - 1},  
311     {CKA_SUBJECT, subject, sizeof(subject)},  
312     {CKA_ID, id, sizeof(id)},  
313     {CKA_SENSITIVE, &>true, sizeof(true)},  
314     {CKA_DERIVE, &>true, sizeof(true)},  
315     {CKA_PRIME, prime, sizeof(prime)},  
316     {CKA_SUBPRIME, subprime, sizeof(subprime)},  
317     {CKA_BASE, base, sizeof(base)},  
318     {CKA_VALUE, value, sizeof(value)}  
319 };
```

## 320 2.2.5 KEA key pair generation

321 The KEA key pair generation mechanism, denoted **CKM\_KEA\_KEY\_PAIR\_GEN**, generates key pairs for  
322 the Key Exchange Algorithm, as defined by NIST’s “SKIPJACK and KEA Algorithm Specification Version  
323 2.0”, 29 May 1998.

324 It does not have a parameter.

325 The mechanism generates KEA public/private key pairs with a particular prime, subprime and base, as  
326 specified in the **CKA\_PRIME**, **CKA\_SUBPRIME**, and **CKA\_BASE** attributes of the template for the public

327 key. Note that this version of Cryptoki does not include a mechanism for generating these KEA domain  
 328 parameters.

329 The mechanism contributes the **CKA\_CLASS**, **CKA\_KEY\_TYPE** and **CKA\_VALUE** attributes to the new  
 330 public key and the **CKA\_CLASS**, **CKA\_KEY\_TYPE**, **CKA\_PRIME**, **CKA\_SUBPRIME**, **CKA\_BASE**, and  
 331 **CKA\_VALUE** attributes to the new private key. Other attributes supported by the KEA public and private  
 332 key types (specifically, the flags indicating which functions the keys support) may also be specified in the  
 333 templates for the keys, or else are assigned default initial values.

334 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
 335 specify the supported range of KEA prime sizes, in bits.

336 **2.2.6 KEA key derivation**

337 The KEA key derivation mechanism, denoted **CKM\_DEA\_DERIVE**, is a mechanism for key derivation  
 338 based on KEA, the Key Exchange Algorithm, as defined by NIST's "SKIPJACK and KEA Algorithm  
 339 Specification Version 2.0", 29 May 1998.

340 It has a parameter, a **CK\_KEA\_DERIVE\_PARAMS** structure.

341 This mechanism derives a secret value, and truncates the result according to the **CKA\_KEY\_TYPE**  
 342 attribute of the template and, if it has one and the key type supports it, the **CKA\_VALUE\_LEN** attribute of  
 343 the template. (The truncation removes bytes from the leading end of the secret value.) The mechanism  
 344 contributes the result as the **CKA\_VALUE** attribute of the new key; other attributes required by the key  
 345 type must be specified in the template.

346 As defined in the Specification, KEA can be used in two different operational modes: full mode and e-mail  
 347 mode. Full mode is a two-phase key derivation sequence that requires real-time parameter exchange  
 348 between two parties. E-mail mode is a one-phase key derivation sequence that does not require real-  
 349 time parameter exchange. By convention, e-mail mode is designated by use of a fixed value of one (1)  
 350 for the KEA parameter  $R_b$  (*pRandomB*).

351 The operation of this mechanism depends on two of the values in the supplied  
 352 **CK\_KEA\_DERIVE\_PARAMS** structure, as detailed in the table below. Note that in all cases, the data  
 353 buffers pointed to by the parameter structure fields *pRandomA* and *pRandomB* must be allocated by the  
 354 caller prior to invoking **C\_DeriveKey**. Also, the values pointed to by *pRandomA* and *pRandomB* are  
 355 represented as Cryptoki "Big integer" data (i.e., a sequence of bytes, most significant byte first).

356 *Table 5, KEA Parameter Values and Operations*

Value of boolean <i>isSender</i>	Value of big integer <i>pRandomB</i>	Token Action (after checking parameter and template values)
CK_TRUE	0	Compute KEA $R_a$ value, store it in <i>pRandomA</i> , return CKR_OK. No derived key object is created.
CK_TRUE	1	Compute KEA $R_a$ value, store it in <i>pRandomA</i> , derive key value using e-mail mode, create key object, return CKR_OK.
CK_TRUE	>1	Compute KEA $R_a$ value, store it in <i>pRandomA</i> , derive key value using full mode, create key object, return CKR_OK
CK_FALSE	0	Compute KEA $R_b$ value, store it in <i>pRandomB</i> , return CKR_OK. No derived key object is created.
CK_FALSE	1	Derive key value using e-mail mode, create key object, return CKR_OK.
CK_FALSE	>1	Derive key value using full mode, create key object, return CKR_OK.

357 Note that the parameter value *pRandomB* == 0 is a flag that the KEA mechanism is being invoked to  
 358 compute the party's public random value ( $R_a$  or  $R_b$ , for sender or recipient, respectively), not to derive a

359 key. In these cases, any object template supplied as the **C\_DeriveKey** *pTemplate* argument should be  
360 ignored.

361 This mechanism has the following rules about key sensitivity and extractability\*:

- 362 • The **CKA\_SENSITIVE** and **CKA\_EXTRACTABLE** attributes in the template for the new key can  
363 both be specified to be either CK\_TRUE or CK\_FALSE. If omitted, these attributes each take on  
364 some default value.
- 365 • If the base key has its **CKA\_ALWAYS\_SENSITIVE** attribute set to CK\_FALSE, then the derived  
366 key will as well. If the base key has its **CKA\_ALWAYS\_SENSITIVE** attribute set to CK\_TRUE,  
367 then the derived has its **CKA\_ALWAYS\_SENSITIVE** attribute set to the same value as its  
368 **CKA\_SENSITIVE** attribute.
- 369 • Similarly, if the base key has its **CKA\_NEVER\_EXTRACTABLE** attribute set to CK\_FALSE, then  
370 the derived key will, too. If the base key has its **CKA\_NEVER\_EXTRACTABLE** attribute set to  
371 CK\_TRUE, then the derived key has its **CKA\_NEVER\_EXTRACTABLE** attribute set to the  
372 *opposite* value from its **CKA\_EXTRACTABLE** attribute.

373 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
374 specify the supported range of KEA prime sizes, in bits.

## 375 2.3 RC2

376 RC2 is a block cipher which is trademarked by RSA Security. It has a variable keysize and an additional  
377 parameter, the “effective number of bits in the RC2 search space”, which can take on values in the range  
378 1-1024, inclusive. The effective number of bits in the RC2 search space is sometimes specified by an  
379 RC2 “version number”; this “version number” is *not* the same thing as the “effective number of bits”,  
380 however. There is a canonical way to convert from one to the other.

### 381 2.3.1 Definitions

382 This section defines the key type “CKK\_RC2” for type CK\_KEY\_TYPE as used in the CKA\_KEY\_TYPE  
383 attribute of key objects.

384 Mechanisms:

- 385 CKM\_RC2\_KEY\_GEN
- 386 CKM\_RC2\_ECB
- 387 CKM\_RC2\_CBC
- 388 CKM\_RC2\_MAC
- 389 CKM\_RC2\_MAC\_GENERAL
- 390 CKM\_RC2\_CBC\_PAD

### 391 2.3.2 RC2 secret key objects

392 RC2 secret key objects (object class **CKO\_SECRET\_KEY**, key type **CKK\_RC2**) hold RC2 keys. The  
393 following table defines the RC2 secret key object attributes, in addition to the common attributes defined  
394 for this object class:

395 *Table 6, RC2 Secret Key Object Attributes*

Attribute	Data type	Meaning
-----------	-----------	---------

\* Note that the rules regarding the **CKA\_SENSITIVE**, **CKA\_EXTRACTABLE**,  
**CKA\_ALWAYS\_SENSITIVE**, and **CKA\_NEVER\_EXTRACTABLE** attributes have changed in version  
2.11 to match the policy used by other key derivation mechanisms such as  
**CKM\_SSL3\_MASTER\_KEY\_DERIVE**.

CKA_VALUE <sup>1,4,6,7</sup>	Byte array	Key value (1 to 128 bytes)
CKA_VALUE_LEN <sup>2,3</sup>	CK_ULONG	Length in bytes of key value

396 Refer to [PKCS #11-Base] table 15 for footnotes

397 The following is a sample template for creating an RC2 secret key object:

```

398 CK_OBJECT_CLASS class = CKO_SECRET_KEY;
399 CK_KEY_TYPE keyType = CKK_RC2;
400 CK_UTF8CHAR label[] = "An RC2 secret key object";
401 CK_BYTE value[] = {...};
402 CK_BBOOL true = CK_TRUE;
403 CK_ATTRIBUTE template[] = {
404     {CKA_CLASS, &class, sizeof(class)},
405     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},
406     {CKA_TOKEN, &>true, sizeof(true)},
407     {CKA_LABEL, label, sizeof(label)-1},
408     {CKA_ENCRYPT, &>true, sizeof(true)},
409     {CKA_VALUE, value, sizeof(value)}
410 };

```

## 411 2.3.3 RC2 mechanism parameters

### 412 2.3.3.1 CK\_RC2\_PARAMS; CK\_RC2\_PARAMS\_PTR

413 **CK\_RC2\_PARAMS** provides the parameters to the **CKM\_RC2\_ECB** and **CKM\_RC2\_MAC** mechanisms.  
414 It holds the effective number of bits in the RC2 search space. It is defined as follows:

```

415 typedef CK_ULONG CK_RC2_PARAMS;

```

416 **CK\_RC2\_PARAMS\_PTR** is a pointer to a **CK\_RC2\_PARAMS**.

### 417 2.3.3.2 CK\_RC2\_CBC\_PARAMS; CK\_RC2\_CBC\_PARAMS\_PTR

418 **CK\_RC2\_CBC\_PARAMS** is a structure that provides the parameters to the **CKM\_RC2\_CBC** and  
419 **CKM\_RC2\_CBC\_PAD** mechanisms. It is defined as follows:

```

420 typedef struct CK_RC2_CBC_PARAMS {
421     CK_ULONG ulEffectiveBits;
422     CK_BYTE iv[8];
423 } CK_RC2_CBC_PARAMS;

```

424 The fields of the structure have the following meanings:

425 *ulEffectiveBits* the effective number of bits in the RC2 search space

426 *iv* the initialization vector (IV) for cipher block chaining  
427 mode

428 **CK\_RC2\_CBC\_PARAMS\_PTR** is a pointer to a **CK\_RC2\_CBC\_PARAMS**.

### 429 2.3.3.3 CK\_RC2\_MAC\_GENERAL\_PARAMS; 430 CK\_RC2\_MAC\_GENERAL\_PARAMS\_PTR

431 **CK\_RC2\_MAC\_GENERAL\_PARAMS** is a structure that provides the parameters to the  
432 **CKM\_RC2\_MAC\_GENERAL** mechanism. It is defined as follows:

```

433 typedef struct CK_RC2_MAC_GENERAL_PARAMS {
434     CK_ULONG ulEffectiveBits;
435     CK_ULONG ulMacLength;
436 } CK_RC2_MAC_GENERAL_PARAMS;

```

437 The fields of the structure have the following meanings:  
 438 *ulEffectiveBits* the effective number of bits in the RC2 search space  
 439 *ulMacLength* length of the MAC produced, in bytes  
 440 **CK\_RC2\_MAC\_GENERAL\_PARAMS\_PTR** is a pointer to a **CK\_RC2\_MAC\_GENERAL\_PARAMS**.

### 441 2.3.4 RC2 key generation

442 The RC2 key generation mechanism, denoted **CKM\_RC2\_KEY\_GEN**, is a key generation mechanism for  
 443 RSA Security's block cipher RC2.

444 It does not have a parameter.

445 The mechanism generates RC2 keys with a particular length in bytes, as specified in the  
 446 **CKA\_VALUE\_LEN** attribute of the template for the key.

447 The mechanism contributes the **CKA\_CLASS**, **CKA\_KEY\_TYPE**, and **CKA\_VALUE** attributes to the new  
 448 key. Other attributes supported by the RC2 key type (specifically, the flags indicating which functions the  
 449 key supports) may be specified in the template for the key, or else are assigned default initial values.

450 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
 451 specify the supported range of RC2 key sizes, in bits.

### 452 2.3.5 RC2-ECB

453 RC2-ECB, denoted **CKM\_RC2\_ECB**, is a mechanism for single- and multiple-part encryption and  
 454 decryption; key wrapping; and key unwrapping, based on RSA Security's block cipher RC2 and electronic  
 455 codebook mode as defined in FIPS PUB 81.

456 It has a parameter, a **CK\_RC2\_PARAMS**, which indicates the effective number of bits in the RC2 search  
 457 space.

458 This mechanism can wrap and unwrap any secret key. Of course, a particular token may not be able to  
 459 wrap/unwrap every secret key that it supports. For wrapping, the mechanism encrypts the value of the  
 460 **CKA\_VALUE** attribute of the key that is wrapped, padded on the trailing end with up to seven null bytes  
 461 so that the resulting length is a multiple of eight. The output data is the same length as the padded input  
 462 data. It does not wrap the key type, key length, or any other information about the key; the application  
 463 must convey these separately.

464 For unwrapping, the mechanism decrypts the wrapped key, and truncates the result according to the  
 465 **CKA\_KEY\_TYPE** attribute of the template and, if it has one, and the key type supports it, the  
 466 **CKA\_VALUE\_LEN** attribute of the template. The mechanism contributes the result as the **CKA\_VALUE**  
 467 attribute of the new key; other attributes required by the key type must be specified in the template.

468 Constraints on key types and the length of data are summarized in the following table:

469 *Table 7 RC2-ECB: Key and Data Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	RC2	Multiple of 8	Same as input length	No final part
C_Decrypt	RC2	Multiple of 8	Same as input length	No final part
C_WrapKey	RC2	Any	Input length rounded up to multiple of 8	
C_UnwrapKey	RC2	Multiple of 8	Determined by type of key being unwrapped or CKA_VALUE_LEN	



470 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
471 specify the supported range of RC2 effective number of bits.

### 472 **2.3.6 RC2-CBC**

473 RC2\_CBC, denoted **CKM\_RC2\_CBC**, is a mechanism for single- and multiple-part encryption and  
474 decryption; key wrapping; and key unwrapping, based on RSA Security's block cipher RC2 and cipher-  
475 block chaining mode as defined in FIPS PUB 81.

476 It has a parameter, a **CK\_RC2\_CBC\_PARAMS** structure, where the first field indicates the effective  
477 number of bits in the RC2 search space, and the next field is the initialization vector for cipher block  
478 chaining mode.

479 This mechanism can wrap and unwrap any secret key. Of course, a particular token may not be able to  
480 wrap/unwrap every secret key that it supports. For wrapping, the mechanism encrypts the value of the  
481 **CKA\_VALUE** attribute of the key that is wrapped, padded on the trailing end with up to seven null bytes  
482 so that the resulting length is a multiple of eight. The output data is the same length as the padded input  
483 data. It does not wrap the key type, key length, or any other information about the key; the application  
484 must convey these separately.

485 For unwrapping, the mechanism decrypts the wrapped key, and truncates the result according to the  
486 **CKA\_KEY\_TYPE** attribute of the template and, if it has one, and the key type supports it, the  
487 **CKA\_VALUE\_LEN** attribute of the template. The mechanism contributes the result as the **CKA\_VALUE**  
488 attribute of the new key; other attributes required by the key type must be specified in the template.

489 Constraints on key types and the length of data are summarized in the following table:

490 *Table 8, RC2-CBC: Key and Data Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	RC2	Multiple of 8	Same as input length	No final part
C_Decrypt	RC2	Multiple of 8	Same as input length	No final part
C_WrapKey	RC2	Any	Input length rounded up to multiple of 8	
C_UnwrapKey	RC2	Multiple of 8	Determined by type of key being unwrapped or CKA_VALUE_LEN	

491 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
492 specify the supported range of RC2 effective number of bits.

### 493 **2.3.7 RC2-CBC with PKCS padding**

494 RC2-CBC with PKCS padding, denoted **CKM\_RC2\_CBC\_PAD**, is a mechanism for single- and multiple-  
495 part encryption and decryption; key wrapping; and key unwrapping, based on RSA Security's block cipher  
496 RC2; cipher-block chaining mode as defined in FIPS PUB 81; and the block cipher padding method  
497 detailed in PKCS #7.

498 It has a parameter, a **CK\_RC2\_CBC\_PARAMS** structure, where the first field indicates the effective  
499 number of bits in the RC2 search space, and the next field is the initialization vector.

500 The PKCS padding in this mechanism allows the length of the plaintext value to be recovered from the  
501 ciphertext value. Therefore, when unwrapping keys with this mechanism, no value should be specified  
502 for the **CKA\_VALUE\_LEN** attribute.

503 In addition to being able to wrap and unwrap secret keys, this mechanism can wrap and unwrap RSA,  
504 Diffie-Hellman, X9.42 Diffie-Hellman, EC (also related to ECDSA) and DSA private keys (see **\*\*\*MISSING**  
505 **REFERENCE\*\*\*** for details). The entries in the table below for data length constraints when wrapping  
506 and unwrapping keys do not apply to wrapping and unwrapping private keys.

507 Constraints on key types and the length of data are summarized in the following table:

508 *Table 9, RC2-CBC with PKCS Padding: Key and Data Length*

Function	Key type	Input length	Output length
C_Encrypt	RC2	Any	Input length rounded up to multiple of 8
C_Decrypt	RC2	Multiple of 8	Between 1 and 8 bytes shorter than input length
C_WrapKey	RC2	Any	Input length rounded up to multiple of 8
C_UnwrapKey	RC2	Multiple of 8	Between 1 and 8 bytes shorter than input length

509 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
510 specify the supported range of RC2 effective number of bits.

### 511 **2.3.8 General-length RC2-MAC**

512 General-length RC2-MAC, denoted **CKM\_RC2\_MAC\_GENERAL**, is a mechanism for single-and  
513 multiple-part signatures and verification, based on RSA Security's block cipher RC2 and data  
514 authorization as defined in FIPS PUB 113.

515 It has a parameter, a **CK\_RC2\_MAC\_GENERAL\_PARAMS** structure, which specifies the effective  
516 number of bits in the RC2 search space and the output length desired from the mechanism.

517 The output bytes from this mechanism are taken from the start of the final RC2 cipher block produced in  
518 the MACing process.

519 Constraints on key types and the length of data are summarized in the following table:

520 *Table 10, General-length RC2-MAC: Key and Data Length*

Function	Key type	Data length	Signature length
C_Sign	RC2	Any	0-8, as specified in parameters
C_Verify	RC2	Any	0-8, as specified in parameters

521 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
522 specify the supported range of RC2 effective number of bits.

### 523 **2.3.9 RC2-MAC**

524 RC2-MAC, denoted by **CKM\_RC2\_MAC**, is a special case of the general-length RC2-MA mechanism  
525 (see Section 2.3.8). Instead of taking a **CK\_RC2\_MAC\_GENERAL\_PARAMS** parameter, it takes a  
526 **CK\_RC2\_PARAMS** parameter, which only contains the effective number of bits in the RC2 search space.  
527 RC2-MAC always produces and verifies 4-byte MACs.

528 Constraints on key types and the length of data are summarized in the following table:

529

530 *Table 11, RC2-MAC: Key and Data Length*

Function	Key type	Data length	Signature length
C_Sign	RC2	Any	4
C_Verify	RC2	Any	4

531 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
532 specify the supported range of RC2 effective number of bits.



## 533 2.4 RC4

### 534 2.4.1 Definitions

535 This section defines the key type “CKK\_RC4” for type CK\_KEY\_TYPE as used in the CKA\_KEY\_TYPE  
536 attribute of key objects.

537 Mechanisms

538 CKM\_RC4\_KEY\_GEN

539 CKM\_RC4

### 540 2.4.2 RC4 secret key objects

541 RC4 secret key objects (object class **CKO\_SECRET\_KEY**, key type **CKK\_RC4**) hold RC4 keys. The  
542 following table defines the RC4 secret key object attributes, in addition to the common attributes defined  
543 for this object class:

544 *Table 12, RC4 Secret Key Object*

Attribute	Data type	Meaning
CKA_VALUE <sup>1,4,6,7</sup>	Byte array	Key value (1 to 256 bytes)
CKA_VALUE_LEN <sup>2,3,6</sup>	CK_ULONG	Length in bytes of key value

545 Refer to [PKCS #11-Base] table 15 for footnotes

546 The following is a sample template for creating an RC4 secret key object:

```
547 CK_OBJECT_CLASS class = CKO_SECRET_KEY;  
548 CK_KEY_TYPE keyType = CKK_RC4;  
549 CK_UTF8CHAR label[] = "An RC4 secret key object";  
550 CK_BYTE value[] = {...};  
551 CK_BBOOL true = CK_TRUE;  
552 CK_ATTRIBUTE template[] = {  
553     {CKA_CLASS, &class, sizeof(class)},  
554     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},  
555     {CKA_TOKEN, &true, sizeof(true)},  
556     {CKA_LABEL, label, sizeof(label)-1},  
557     {CKA_ENCRYPT, &true, sizeof(true)},  
558     {CKA_VALUE, value, sizeof(value)}  
559 };
```

### 560 2.4.3 RC4 key generation

561 The RC4 key generation mechanism, denoted **CKM\_RC4\_KEY\_GEN**, is a key generation mechanism for  
562 RSA Security's proprietary stream cipher RC4.

563 It does not have a parameter.

564 The mechanism generates RC4 keys with a particular length in bytes, as specified in the  
565 **CKA\_VALUE\_LEN** attribute of the template for the key.

566 The mechanism contributes the **CKA\_CLASS**, **CKA\_KEY\_TYPE**, and **CKA\_VALUE** attributes to the new  
567 key. Other attributes supported by the RC4 key type (specifically, the flags indicating which functions the  
568 key supports) may be specified in the template for the key, or else are assigned default initial values.

569 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
570 specify the supported range of RC4 key sizes, in bits.

571 **2.4.4 RC4 mechanism**

572 RC4, denoted **CKM\_RC4**, is a mechanism for single- and multiple-part encryption and decryption based  
573 on RSA Security's proprietary stream cipher RC4.

574 It does not have a parameter.

575 Constraints on key types and the length of input and output data are summarized in the following table:

576 *Table 13, RC4: Key and Data Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	RC4	Any	Same as input length	No final part
C_Decrypt	RC4	Any	Same as input length	No final part

577 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
578 specify the supported range of RC4 key sizes, in bits.

579 **2.5 RC5**

580 RC5 is a parameterizable block cipher patented by RSA Security. It has a variable wordsize, a variable  
581 keysize, and a variable number of rounds. The blocksize of RC5 is always equal to twice its wordsize.

582 **2.5.1 Definitions**

583 This section defines the key type "CKK\_RC5" for type CK\_KEY\_TYPE as used in the CKA\_KEY\_TYPE  
584 attribute of key objects.

585 Mechanisms:

- 586 CKM\_RC5\_KEY\_GEN
- 587 CKM\_RC5\_ECB
- 588 CKM\_RC5\_CBC
- 589 CKM\_RC5\_MAC
- 590 CKM\_RC5\_MAC\_GENERAL
- 591 CMK\_RC5\_CBC\_PAD

592 **2.5.2 RC5 secret key objects**

593 RC5 secret key objects (object class **CKO\_SECRET\_KEY**, key type **CKK\_RC5**) hold RC5 keys. The  
594 following table defines the RC5 secret key object attributes, in addition to the common attributes defined  
595 for this object class.

596 *Table 14, RC5 Secret Key Object*

Attribute	Data type	Meaning
CKA_VALUE <sup>1,4,6,7</sup>	Byte array	Key value (0 to 255 bytes)
CKA_VALUE_LEN <sup>2,3,6</sup>	CK_ULONG	Length in bytes of key value

597 Refer to [PKCS #11-Base] table 15 for footnotes

598

599 The following is a sample template for creating an RC5 secret key object:

```
600 CK_OBJECT_CLASS class = CKO_SECRET_KEY;  
601 CK_KEY_TYPE keyType = CKK_RC5;  
602 CK_UTF8CHAR label[] = "An RC5 secret key object";  
603 CK_BYTE value[] = {...};  
604 CK_BBOOL true = CK_TRUE;
```

```

605 CK_ATTRIBUTE template[] = {
606     {CKA_CLASS, &class, sizeof(class)},
607     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},
608     {CKA_TOKEN, &>true, sizeof(true)},
609     {CKA_LABEL, label, sizeof(label)-1},
610     {CKA_ENCRYPT, &>true, sizeof(true)},
611     {CKA_VALUE, value, sizeof(value)}
612 };

```

## 613 2.5.3 RC5 mechanism parameters

### 614 2.5.3.1 CK\_RC5\_PARAMS; CK\_RC5\_PARAMS\_PTR

615 **CK\_RC5\_PARAMS** provides the parameters to the **CKM\_RC5\_ECB** and **CKM\_RC5\_MAC** mechanisms.  
616 It is defined as follows:

```

617 typedef struct CK_RC5_PARAMS {
618     CK_ULONG ulWordsize;
619     CK_ULONG ulRounds;
620 } CK_RC5_PARAMS;

```

621 The fields of the structure have the following meanings:

622 *ulWordsize*      wordsize of RC5 cipher in bytes

623 *ulRounds*        number of rounds of RC5 encipherment

624 **CK\_RC5\_PARAMS\_PTR** is a pointer to a **CK\_RC5\_PARAMS**.

### 625 2.5.3.2 CK\_RC5\_CBC\_PARAMS; CK\_RC5\_CBC\_PARAMS\_PTR

626 **CK\_RC5\_CBC\_PARAMS** is a structure that provides the parameters to the **CKM\_RC5\_CBC** and  
627 **CKM\_RC5\_CBC\_PAD** mechanisms. It is defined as follows:

```

628 typedef struct CK_RC5_CBC_PARAMS {
629     CK_ULONG ulWordsize;
630     CK_ULONG ulRounds;
631     CK_BYTE_PTR pIV;
632     CK_ULONG ulIVLen;
633 } CK_RC5_CBC_PARAMS;

```

634 The fields of the structure have the following meanings:

635 *ulwordSize*      wordsize of RC5 cipher in bytes

636 *ulRounds*        number of rounds of RC5 encipherment

637 *pIV*              pointer to initialization vector (IV) for CBC encryption

638 *ulIVLen*         length of initialization vector (must be same as  
639                      blocksize)

640 **CK\_RC5\_CBC\_PARAMS\_PTR** is a pointer to a **CK\_RC5\_CBC\_PARAMS**.

### 641 2.5.3.3 CK\_RC5\_MAC\_GENERAL\_PARAMS; 642 CK\_RC5\_MAC\_GENERAL\_PARAMS\_PTR

643 **CK\_RC5\_MAC\_GENERAL\_PARAMS** is a structure that provides the parameters to the  
644 **CKM\_RC5\_MAC\_GENERAL** mechanism. It is defined as follows:

```

645 typedef struct CK_RC5_MAC_GENERAL_PARAMS {
646     CK_ULONG ulWordsize;
647     CK_ULONG ulRounds;
648     CK_ULONG ulMacLength;
649 } CK_RC5_MAC_GENERAL_PARAMS;

```

650 The fields of the structure have the following meanings:

- 651 *ulwordSize*      wordsize of RC5 cipher in bytes
- 652 *ulRounds*        number of rounds of RC5 encipherment
- 653 *ulMacLength*     length of the MAC produced, in bytes

654 **CK\_RC5\_MAC\_GENERAL\_PARAMS\_PTR** is a pointer to a **CK\_RC5\_MAC\_GENERAL\_PARAMS**.

### 655 2.5.4 RC5 key generation

656 The RC5 key generation mechanism, denoted **CKM\_RC5\_KEY\_GEN**, is a key generation mechanism for  
657 RSA Security's block cipher RC5.

658 It does not have a parameter.

659 The mechanism generates RC5 keys with a particular length in bytes, as specified in the  
660 **CKA\_VALUE\_LEN** attribute of the template for the key.

661 The mechanism contributes the **CKA\_CLASS**, **CKA\_KEY\_TYPE**, and **CKA\_VALUE** attributes to the new  
662 key. Other attributes supported by the RC5 key type (specifically, the flags indicating which functions the  
663 key supports) may be specified in the template for the key, or else are assigned default initial values.

664 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
665 specify the supported range of RC5 key sizes, in bytes.

### 666 2.5.5 RC5-ECB

667 RC5-ECB, denoted **CKM\_RC5\_ECB**, is a mechanism for single- and multiple-part encryption and  
668 decryption; key wrapping; and key unwrapping, based on RSA Security's block cipher RC5 and electronic  
669 codebook mode as defined in FIPS PUB 81.

670 It has a parameter, **CK\_RC5\_PARAMS**, which indicates the wordsize and number of rounds of  
671 encryption to use.

672 This mechanism can wrap and unwrap any secret key. Of course, a particular token may not be able to  
673 wrap/unwrap every secret key that it supports. For wrapping, the mechanism encrypts the value of the  
674 **CKA\_VALUE** attribute of the key that is wrapped, padded on the trailing end with null bytes so that the  
675 resulting length is a multiple of the cipher blocksize (twice the wordsize). The output data is the same  
676 length as the padded input data. It does not wrap the key type, key length, or any other information about  
677 the key; the application must convey these separately.

678 For unwrapping, the mechanism decrypts the wrapped key, and truncates the result according to the  
679 **CKA\_KEY\_TYPE** attributes of the template and, if it has one, and the key type supports it, the  
680 **CKA\_VALUE\_LEN** attribute of the template. The mechanism contributes the result as the **CKA\_VALUE**  
681 attribute of the new key; other attributes required by the key type must be specified in the template.

682 Constraints on key types and the length of data are summarized in the following table:

683 *Table 15, RC5-ECB Key and Data Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	RC5	Multiple of blocksize	Same as input length	No final part

C_Decrypt	RC5	Multiple of blocksize	Same as input length	No final part
C_WrapKey	RC5	Any	Input length rounded up to multiple of blocksize	
C_UnwrapKey	RC5	Multiple of blocksize	Determined by type of key being unwrapped or CKA_VALUE_LEN	

684 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
685 specify the supported range of RC5 key sizes, in bytes.

## 686 2.5.6 RC5-CBC

687 RC5-CBC, denoted **CKM\_RC5\_CBC**, is a mechanism for single- and multiple-part encryption and  
688 decryption; key wrapping; and key unwrapping, based on RSA Security's block cipher RC5 and cipher-  
689 block chaining mode as defined in FIPS PUB 81.

690 It has a parameter, a **CK\_RC5\_CBC\_PARAMS** structure, which specifies the wordsize and number of  
691 rounds of encryption to use, as well as the initialization vector for cipher block chaining mode.

692 This mechanism can wrap and unwrap any secret key. Of course, a particular token may not be able to  
693 wrap/unwrap every secret key that it supports. For wrapping, the mechanism encrypts the value of the  
694 **CKA\_VALUE** attribute of the key that is wrapped, padded on the trailing end with up to seven null bytes  
695 so that the resulting length is a multiple of eight. The output data is the same length as the padded input  
696 data. It does not wrap the key type, key length, or any other information about the key; the application  
697 must convey these separately.

698 For unwrapping, the mechanism decrypts the wrapped key, and truncates the result according to the  
699 **CKA\_KEY\_TYPE** attribute for the template, and, if it has one, and the key type supports it, the  
700 **CKA\_VALUE\_LEN** attribute of the template. The mechanism contributes the result as the **CKA\_VALUE**  
701 attribute of the new key; other attributes required by the key type must be specified in the template.

702 Constraints on key types and the length of data are summarized in the following table:

703 *Table 16, RC5-CBC Key and Data Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	RC5	Multiple of blocksize	Same as input length	No final part
C_Decrypt	RC5	Multiple of blocksize	Same as input length	No final part
C_WrapKey	RC5	Any	Input length rounded up to multiple of blocksize	
C_UnwrapKey	RC5	Multiple of blocksize	Determined by type of key being unwrapped or CKA_VALUE_LEN	

704 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
705 specify the supported range of RC5 key sizes, in bytes.

## 706 2.5.7 RC5-CBC with PKCS padding

707 RC5-CBC with PKCS padding, denoted **CKM\_RC5\_CBC\_PAD**, is a mechanism for single- and multiple-  
708 part encryption and decryption; key wrapping; and key unwrapping, based on RSA Security's block cipher  
709 RC5; cipher block chaining mode as defined in FIPS PUB 81; and the block cipher padding method  
710 detailed in PKCS #7.

711 It has a parameter, a **CK\_RC5\_CBC\_PARAMS** structure, which specifies the wordsize and number of  
 712 rounds of encryption to use, as well as the initialization vector for cipher block chaining mode.

713 The PKCS padding in this mechanism allows the length of the plaintext value to be recovered from the  
 714 ciphertext value. Therefore, when unwrapping keys with this mechanism, no value should be specified  
 715 for the **CKA\_VALUE\_LEN** attribute.

716 In addition to being able to wrap an unwrap secret keys, this mechanism can wrap and unwrap RSA,  
 717 Diffie-Hellman, X9.42 Diffie-Hellman, EC (also related to ECDSA) and DSA private keys (see Section  
 718 **\*\*\*MISSING REFERENCE\*\*\*** for details). The entries in the table below for data length constraints when  
 719 wrapping and unwrapping keys do not apply to wrapping and unwrapping private keys.

720 Constraints on key types and the length of data are summarized in the following table:

721 *Table 17, RC5-CBC with PKCS Padding; Key and Data Length*

Function	Key type	Input length	Output length
C_Encrypt	RC5	Any	Input length rounded up to multiple of blocksize
C_Decrypt	RC5	Multiple of blocksize	Between 1 and blocksize bytes shorter than input length
C_WrapKey	RC5	Any	Input length rounded up to multiple of blocksize
C_UnwrapKey	RC5	Multiple of blocksize	Between 1 and blocksize bytes shorter than input length

722 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
 723 specify the supported range of RC5 key sizes, in bytes.

## 724 **2.5.8 General-length RC5-MAC**

725 General-length RC5-MAC, denoted **CKM\_RC5\_MAC\_GENERAL**, is a mechanism for single- and  
 726 multiple-part signatures and verification, based on RSA Security's block cipher RC5 and data  
 727 authentication as defined in FIPS PUB 113.

728 It has a parameter, a **CK\_RC5\_MAC\_GENERAL\_PARAMS** structure, which specifies the wordsize and  
 729 number of rounds of encryption to use and the output length desired from the mechanism.

730 The output bytes from this mechanism are taken from the start of the final RC5 cipher block produced in  
 731 the MACing process.

732 Constraints on key types and the length of data are summarized in the following table:

733 *Table 18, General-length RC2-MAC: Key and Data Length*

Function	Key type	Data length	Signature length
C_Sign	RC5	Any	0-blocksize, as specified in parameters
C_Verify	RC5	Any	0-blocksize, as specified in parameters

734 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
 735 specify the supported range of RC5 key sizes, in bytes.

## 736 **2.5.9 RC5-MAC**

737 RC5-MAC, denoted by **CKM\_RC5\_MAC**, is a special case of the general-length RC5-MAC mechanism.  
 738 Instead of taking a **CK\_RC5\_MAC\_GENERAL\_PARAMS** parameter, it takes a **CK\_RC5\_PARAMS**  
 739 parameter. RC5-MAC always produces and verifies MACs half as large as the RC5 blocksize.

740 Constraints on key types and the length of data are summarized in the following table:

741 *Table 19, RC5-MAC: Key and Data Length*

Function	Key type	Data length	Signature length
C_Sign	RC5	Any	RC5 wordsize = [blocksize/2]
C_Verify	RC5	Any	RC5 wordsize = [blocksize/2]

742 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
743 specify the supported range of RC5 key sizes, in bytes.

## 744 2.6 General block cipher

745 For brevity's sake, the mechanisms for the DES, CAST, CAST3, CAST128 (CAST5), IDEA and CDMF  
746 block ciphers will be described together here. Each of these ciphers has the following mechanisms, which  
747 will be described in a templated form.

### 748 2.6.1 Definitions

749 This section defines the key types "CKK\_DES", "CKK\_CAST", "CKK\_CAST3", "CKK\_CAST5"  
750 (deprecated in v2.11), "CKK\_CAST128", "CKK\_IDEA" and "CKK\_CDMF" for type CK\_KEY\_TYPE as  
751 used in the CKA\_KEY\_TYPE attribute of key objects.

752 Mechanisms:

753 CKM\_DES\_KEY\_GEN  
754 CKM\_DES\_ECB  
755 CKM\_DES\_CBC  
756 CKM\_DES\_MAC  
757 CKM\_DES\_MAC\_GENERAL  
758 CKM\_DES\_CBC\_PAD  
759 CKM\_CDMF\_KEY\_GEN  
760 CKM\_CDMF\_ECB  
761 CKM\_CDMF\_CBC  
762 CKM\_CDMF\_MAC  
763 CKM\_CDMF\_MAC\_GENERAL  
764 CKM\_CDMF\_CBC\_PAD  
765 CKM\_DES\_OFB64  
766 CKM\_DES\_OFB8  
767 CKM\_DES\_CFB64  
768 CKM\_DES\_CFB8  
769 CKM\_CAST\_KEY\_GEN  
770 CKM\_CAST\_ECB  
771 CKM\_CAST\_CBC  
772 CKM\_CAST\_MAC  
773 CKM\_CAST\_MAC\_GENERAL  
774 CKM\_CAST\_CBC\_PAD  
775 CKM\_CAST3\_KEY\_GEN  
776 CKM\_CAST3\_ECB  
777 CKM\_CAST3\_CBC  
778 CKM\_CAST3\_MAC  
779 CKM\_CAST3\_MAC\_GENERAL



780 CKM\_CAST3\_CBC\_PAD  
 781 CKM\_CAST5\_KEY\_GEN  
 782 CKM\_CAST128\_KEY\_GEN  
 783 CKM\_CAST5\_ECB  
 784 CKM\_CAST128\_ECB  
 785 CKM\_CAST5\_CBC  
 786 CKM\_CAST128\_CBC  
 787 CKM\_CAST5\_MAC  
 788 CKM\_CAST128\_MAC  
 789 CKM\_CAST5\_MAC\_GENERAL  
 790 CKM\_CAST128\_MAC\_GENERAL  
 791 CKM\_CAST5\_CBC\_PAD  
 792 CKM\_CAST128\_CBC\_PAD  
 793 CKM\_IDEA\_KEY\_GEN  
 794 CKM\_IDEA\_ECB  
 795 CKM\_IDEA\_MAC  
 796 CKM\_IDEA\_MAC\_GENERAL  
 797 CKM\_IDEA\_CBC\_PAD

798 **2.6.2 DES secret key objects**

799 DES secret key objects (object class **CKO\_SECRET\_KEY**, key type **CKK\_DES**) hold single-length DES  
 800 keys. The following table defines the DES secret key object attributes, in addition to the common  
 801 attributes defined for this object class:

802 *Table 20, DES Secret Key Object*

Attribute	Data type	Meaning
CKA_VALUE <sup>1,4,6,7</sup>	Byte array	Key value (always 8 bytes long)

803 Refer to [PKCS #11-Base] table 15 for footnotes

804 DES keys must always have their parity bits properly set as described in FIPS PUB 46-3. Attempting to  
 805 create or unwrap a DES key with incorrect parity will return an error.

806 The following is a sample template for creating a DES secret key object:

```
807 CK_OBJECT_CLASS class = CKO_SECRET_KEY;
808 CK_KEY_TYPE keyType = CKK_DES;
809 CK_UTF8CHAR label[] = "A DES secret key object";
810 CK_BYTE value[8] = {...};
811 CK_BBOOL true = CK_TRUE;
812 CK_ATTRIBUTE template[] = {
813     {CKA_CLASS, &class, sizeof(class)},
814     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},
815     {CKA_TOKEN, &>true, sizeof(true)},
816     {CKA_LABEL, label, sizeof(label)-1},
817     {CKA_ENCRYPT, &>true, sizeof(true)},
818     {CKA_VALUE, value, sizeof(value)}
819 };
```

820 CKA\_CHECK\_VALUE: The value of this attribute is derived from the key object by taking the first three  
 821 bytes of the ECB encryption of a single block of null (0x00) bytes, using the default cipher associated with  
 822 the key type of the secret key object.



823 **2.6.3 CAST secret key objects**

824 CAST secret key objects (object class **CKO\_SECRET\_KEY**, key type **CKK\_CAST**) hold CAST keys.  
825 The following table defines the CAST secret key object attributes, in addition to the common attributes  
826 defined for this object class:

827 *Table 21, CAST Secret Key Object Attributes*

Attribute	Data type	Meaning
CKA_VALUE <sup>1,4,6,7</sup>	Byte array	Key value (1 to 8 bytes)
CKA_VALUE_LEN <sup>2,3,6</sup>	CK_ULONG	Length in bytes of key value

828 Refer to [PKCS #11-Base] table 15 for footnotes

829

830 The following is a sample template for creating a CAST secret key object:

```

831 CK_OBJECT_CLASS class = CKO_SECRET_KEY;
832 CK_KEY_TYPE keyType = CKK_CAST;
833 CK_UTF8CHAR label[] = "A CAST secret key object";
834 CK_BYTE value[] = {...};
835 CK_BBOOL true = CK_TRUE;
836 CK_ATTRIBUTE template[] = {
837     {CKA_CLASS, &class, sizeof(class)},
838     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},
839     {CKA_TOKEN, &>true, sizeof(true)},
840     {CKA_LABEL, label, sizeof(label)-1},
841     {CKA_ENCRYPT, &>true, sizeof(true)},
842     {CKA_VALUE, value, sizeof(value)}
843 };

```

844 **2.6.4 CAST3 secret key objects**

845 CAST3 secret key objects (object class **CKO\_SECRET\_KEY**, key type **CKK\_CAST3**) hold CAST3 keys.  
846 The following table defines the CAST3 secret key object attributes, in addition to the common attributes  
847 defines for this object class:

848 *Table 22, CAST3 Secret Key Object Attributes*

Attribute	Data type	Meaning
CKA_VALUE <sup>1,4,6,7</sup>	Byte array	Key value (1 to 8 bytes)
CKA_VALUE_LEN <sup>2,3,6</sup>	CK_ULONG	Length in bytes of key value

849 Refer to [PKCS #11-Base] table 15 for footnotes

850 The following is a sample template for creating a CAST3 secret key object:

```

851 CK_OBJECT_CLASS class = CKO_SECRET_KEY;
852 CK_KEY_TYPE keyType = CKK_CAST3;
853 CK_UTF8CHAR label[] = "A CAST3 secret key object";
854 CK_BYTE value[] = {...};
855 CK_BBOOL true = CK_TRUE;
856 CK_ATTRIBUTE template[] = {
857     {CKA_CLASS, &class, sizeof(class)},
858     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},
859     {CKA_TOKEN, &>true, sizeof(true)},
860     {CKA_LABEL, label, sizeof(label)-1},
861     {CKA_ENCRYPT, &>true, sizeof(true)},
862     {CKA_VALUE, value, sizeof(value)}
863 };

```

## 864 2.6.5 CAST128 (CAST5) secret key objects

865 CAST128 (also known as CAST5) secret key objects (object class **CKO\_SECRET\_KEY**, key type  
866 **CKK\_CAST128** or **CKK\_CAST5**) hold CAST128 keys. The following table defines the CAST128 secret  
867 key object attributes, in addition to the common attributes defines for this object class:

868 Table 23, CAST128 (CAST5) Secret Key Object Attributes

Attribute	Data type	Meaning
CKA_VALUE <sup>1,4,6,7</sup>	Byte array	Key value (1 to 16 bytes)
CKA_VALUE_LEN <sup>2,3,6</sup>	CK_ULONG	Length in bytes of key value

869 Refer to [PKCS #11-Base] table 15 for footnotes

870 The following is a sample template for creating a CAST128 (CAST5) secret key object:

```
871 CK_OBJECT_CLASS class = CKO_SECRET_KEY;  
872 CK_KEY_TYPE keyType = CKK_CAST128;  
873 CK_UTF8CHAR label[] = "A CAST128 secret key object";  
874 CK_BYTE value[] = {...};  
875 CK_BBOOL true = CK_TRUE;  
876 CK_ATTRIBUTE template[] = {  
877     {CKA_CLASS, &class, sizeof(class)},  
878     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},  
879     {CKA_TOKEN, &>true, sizeof(true)},  
880     {CKA_LABEL, label, sizeof(label)-1},  
881     {CKA_ENCRYPT, &>true, sizeof(true)},  
882     {CKA_VALUE, value, sizeof(value)}  
883 };
```

884

## 885 2.6.6 IDEA secret key objects

886 IDEA secret key objects (object class **CKO\_SECRET\_KEY**, key type **CKK\_IDEA**) hold IDEA keys. The following  
887 table defines the IDEA secret key object attributes, in addition to the common attributes defines for this object class:

888 Table 24, IDEA Secret Key Object

Attribute	Data type	Meaning
CKA_VALUE <sup>1,4,6,7</sup>	Byte array	Key value (always 16 bytes long)

889 Refer to [PKCS #11-Base] table 15 for footnotes

890 The following is a sample template for creating an IDEA secret key object:

```
891 CK_OBJECT_CLASS class = CKO_SECRET_KEY;  
892 CK_KEY_TYPE keyType = CKK_IDEA;  
893 CK_UTF8CHAR label[] = "An IDEA secret key object";  
894 CK_BYTE value[16] = {...};  
895 CK_BBOOL true = CK_TRUE;  
896 CK_ATTRIBUTE template[] = {  
897     {CKA_CLASS, &class, sizeof(class)},  
898     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},  
899     {CKA_TOKEN, &>true, sizeof(true)},  
900     {CKA_LABEL, label, sizeof(label)-1},  
901     {CKA_ENCRYPT, &>true, sizeof(true)},  
902     {CKA_VALUE, value, sizeof(value)}  
903 };
```

904

## 905 2.6.7 CDMF secret key objects

906 *IDEA secret key objects (object class **CKO\_SECRET\_KEY**, key type **CKK\_CDMF**) hold CDMF keys. The following*  
907 *table defines the CDMF secret key object attributes, in addition to the common attributes defines for this object class:*

908 *Table 25, CDMF Secret Key Object*

Attribute	Data type	Meaning
CKA_VALUE <sup>1,4,6,7</sup>	Byte array	Key value (always 8 bytes long)

909 Refer to [PKCS #11-Base] table 15 for footnotes

910 CDMF keys must always have their parity bits properly set in exactly the same fashion described for DES  
911 keys in FIPS PUB 46-3. Attempting to create or unwrap a CDMF key with incorrect parity will return an  
912 error.

913 The following is a sample template for creating a CDMF secret key object:

```
914 CK_OBJECT_CLASS class = CKO_SECRET_KEY;  
915 CK_KEY_TYPE keyType = CKK_CDMF;  
916 CK_UTF8CHAR label[] = "A CDMF secret key object";  
917 CK_BYTE value[8] = {...};  
918 CK_BBOOL true = CK_TRUE;  
919 CK_ATTRIBUTE template[] = {  
920     {CKA_CLASS, &class, sizeof(class)},  
921     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},  
922     {CKA_TOKEN, &>true, sizeof(true)},  
923     {CKA_LABEL, label, sizeof(label)-1},  
924     {CKA_ENCRYPT, &true, sizeof(true)},  
925     {CKA_VALUE, value, sizeof(value)}  
926 };
```

## 927 2.6.8 General block cipher mechanism parameters

### 928 2.6.8.1 CK\_MAC\_GENERAL\_PARAMS; CK\_MAC\_GENERAL\_PARAMS\_PTR

929 **CK\_MAC\_GENERAL\_PARAMS** provides the parameters to the general-length MACing mechanisms of  
930 the DES, DES3 (triple-DES), CAST, CAST3, CAST128 (CAST5), IDEA, CDMF and AES ciphers. It also  
931 provides the parameters to the general-length HMACing mechanisms (i.e., MD2, MD5, SHA-1, SHA-256,  
932 SHA-384, SHA-512, RIPEMD-128 and RIPEMD-160) and the two SSL 3.0 MACing mechanisms, (i.e.,  
933 MD5 and SHA-1). It holds the length of the MAC that these mechanisms will produce. It is defined as  
934 follows:

```
935 typedef CK_ULONG CK_MAC_GENERAL_PARAMS;  
936
```

937 **CK\_MAC\_GENERAL\_PARAMS\_PTR** is a pointer to a **CK\_MAC\_GENERAL\_PARAMS**.

## 938 2.6.9 General block cipher key generation

939 Cipher <NAME> has a key generation mechanism, "<NAME> key generation", denoted by  
940 **CKM\_<NAME>\_KEY\_GEN**.

941 This mechanism does not have a parameter.

942 The mechanism contributes the **CKA\_CLASS**, **CKA\_KEY\_TYPE**, and **CKA\_VALUE** attributes to the new  
943 key. Other attributes supported by the key type (specifically, the flags indicating which functions the key  
944 supports) may be specified in the template for the key, or else are assigned default initial values.

945 When DES keys or CDMF keys are generated, their parity bits are set properly, as specified in FIPS PUB  
946 46-3. Similarly, when a triple-DES key is generated, each of the DES keys comprising it has its parity bits  
947 set properly.

948 When DES or CDMF keys are generated, it is token-dependent whether or not it is possible for “weak” or  
 949 “semi-weak” keys to be generated. Similarly, when triple-DES keys are generated, it is token-dependent  
 950 whether or not it is possible for any of the component DES keys to be “weak” or “semi-weak” keys.

951 When CAST, CAST3, or CAST128 (CAST5) keys are generated, the template for the secret key must  
 952 specify a **CKA\_VALUE\_LEN** attribute.

953 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
 954 may or may not be used. The CAST, CAST3, and CAST128 (CAST5) ciphers have variable key sizes,  
 955 and so for the key generation mechanisms for these ciphers, the *ulMinKeySize* and *ulMaxKeySize* fields  
 956 of the **CK\_MECHANISM\_INFO** structure specify the supported range of key sizes, in bytes. For the DES,  
 957 DES3 (triple-DES), IDEA and CDMF ciphers, these fields and not used.

## 958 2.6.10 General block cipher ECB

959 Cipher <NAME> has an electronic codebook mechanism, “<NAME>-ECB”, denoted  
 960 **CKM\_<NAME>\_ECB**. It is a mechanism for single- and multiple-part encryption and decryption; key  
 961 wrapping; and key unwrapping with <NAME>.

962 It does not have a parameter.

963 This mechanism can wrap and unwrap any secret key. Of course, a particular token may not be able to  
 964 wrap/unwrap every secret key that it supports. For wrapping, the mechanism encrypts the value of the  
 965 **CKA\_VALUE** attribute of the key that is wrapped, padded on the trailing end with null bytes so that the  
 966 resulting length is a multiple of <NAME>’s blocksize. The output data is the same length as the padded  
 967 input data. It does not wrap the key type, key length or any other information about the key; the  
 968 application must convey these separately.

969 For unwrapping, the mechanism decrypts the wrapped key, and truncates the result according to the  
 970 **CKA\_KEY\_TYPE** attribute of the template and, if it has one, and the key type supports it, the  
 971 **CKA\_VALUE\_LEN** attribute of the template. The mechanism contributes the result as the **CKA\_VALUE**  
 972 attribute of the new key; other attributes required by the key must be specified in the template.

973 Constraints on key types and the length of data are summarized in the following table:

974 *Table 26, General Block Cipher ECB: Key and Data Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	<NAME>	Multiple of blocksize	Same as input length	No final part
C_Decrypt	<NAME>	Multiple of blocksize	Same as input length	No final part
C_WrapKey	<NAME>	Any	Input length rounded up to multiple of blocksize	
C_UnwrapKey	<NAME>	Any	Determined by type of key being unwrapped or CKA_VALUE_LEN	

975 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
 976 may or may not be used. The CAST, CAST3, and CAST128 (CAST5) ciphers have variable key sizes,  
 977 and so for these ciphers, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO**  
 978 structure specify the supported range of key sizes, in bytes. For the DES, DES3 (triple-DES), IDEA and  
 979 CDMF ciphers, these fields are not used.

## 980 2.6.11 General block cipher CBC

981 Cipher <NAME> has a cipher-block chaining mode, “<NAME>-CBC”, denoted **CKM\_<NAME>\_CBC**. It is  
 982 a mechanism for single- and multiple-part encryption and decryption; key wrapping; and key unwrapping  
 983 with <NAME>.

984 It has a parameter, an initialization vector for cipher block chaining mode. The initialization vector has the  
 985 same length as <NAME>'s blocksize.

986 Constraints on key types and the length of data are summarized in the following table:

987 *Table 27, General Block Cipher CBC; Key and Data Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	<NAME>	Multiple of blocksize	Same as input length	No final part
C_Decrypt	<NAME>	Multiple of blocksize	Same as input length	No final part
C_WrapKey	<NAME>	Any	Input length rounded up to multiple of blocksize	
C_UnwrapKey	<NAME>	Any	Determined by type of key being unwrapped or CKA_VALUE_LEN	

988 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
 989 may or may not be used. The CAST, CAST3, and CAST128 (CAST5) ciphers have variable key sizes,  
 990 and so for these ciphers, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO**  
 991 structure specify the supported range of key sizes, in bytes. For the DES, DES3 (triple-DES), IDEA, and  
 992 CDMF ciphers, these fields are not used.

### 993 **2.6.12 General block cipher CBC with PKCS padding**

994 Cipher <NAME> has a cipher-block chaining mode with PKCS padding, “<NAME>-CBC with PKCS  
 995 padding”, denoted **CKM\_<NAME>\_CBC\_PAD**. It is a mechanism for single- and multiple-part encryption  
 996 and decryption; key wrapping; and key unwrapping with <NAME>. All ciphertext is padded with PKCS  
 997 padding.

998 It has a parameter, an initialization vector for cipher block chaining mode. The initialization vector has the  
 999 same length as <NAME>'s blocksize.

1000 The PKCS padding in this mechanism allows the length of the plaintext value to be recovered from the  
 1001 ciphertext value. Therefore, when unwrapping keys with this mechanism, no value should be specified  
 1002 for the **CKA\_VALUE\_LEN** attribute.

1003

1004 In addition to being able to wrap and unwrap secret keys, this mechanism can wrap and unwrap RSA,  
 1005 Diffie-Hellman, X9.42 Diffie-Hellman, EC (also related to ECDSA) and DSA private keys (see Section  
 1006 **\*\*\*MISSING REFERENCE\*\*\*** for details). The entries in the table below for data length constraints when  
 1007 wrapping and unwrapping keys to not apply to wrapping and unwrapping private keys.

1008 Constraints on key types and the length of data are summarized in the following table:

1009 *Table 28, General Block Cipher CBC with PKCS Padding: Key and Data Length*

Function	Key type	Input length	Output length
C_Encrypt	<NAME>	Any	Input length rounded up to multiple of blocksize
C_Decrypt	<NAME>	Multiple of blocksize	Between 1 and blocksize bytes shorter than input length
C_WrapKey	<NAME>	Any	Input length rounded up to multiple of blocksize
C_UnwrapKey	<NAME>	Multiple of	Between 1 and blocksize bytes shorter than input

		blocksize	length
--	--	-----------	--------

1010 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
1011 may or may not be used. The CAST, CAST3 and CAST128 (CAST5) ciphers have variable key sizes,  
1012 and so for these ciphers, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO**  
1013 structure specify the supported range of key sizes, in bytes. For the DES, DES3 (triple-DES), IDEA, and  
1014 CDMF ciphers, these fields are not used.

### 1015 2.6.13 General-length general block cipher MAC

1016 Cipher <NAME> has a general-length MACing mode, “General-length <NAME>-MAC”, denoted  
1017 **CKM\_<NAME>\_MAC\_GENERAL**. It is a mechanism for single-and multiple-part signatures and  
1018 verification, based on the <NAME> encryption algorithm and data authentication as defined in FIPS PUB  
1019 113.

1020 It has a parameter, a **CK\_MAC\_GENERAL\_PARAMS**, which specifies the size of the output.

1021 The output bytes from this mechanism are taken from the start of the final cipher block produced in the  
1022 MACing process.

1023 Constraints on key types and the length of input and output data are summarized in the following table:

1024 *Table 29, General-length General Block Cipher MAC: Key and Data Length*

Function	Key type	Data length	Signature length
C_Sign	<NAME>	Any	0-blocksize, depending on parameters
C_Verify	<NAME>	Any	0-blocksize, depending on parameters

1025 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
1026 may or may not be used. The CAST, CAST3, and CAST128 (CAST5) ciphers have variable key sizes,  
1027 and so for these ciphers, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO**  
1028 structure specify the supported range of key sizes, in bytes. For the DES, DES3 (triple-DES), IDEA and  
1029 CDMF ciphers, these fields are not used.

### 1030 2.6.14 General block cipher MAC

1031 Cipher <NAME> has a MACing mechanism, “<NAME>-MAC”, denoted **CKM\_<NAME>\_MAC**. This  
1032 mechanism is a special case of the **CKM\_<NAME>\_MAC\_GENERAL** mechanism described above. It  
1033 always produces an output of size half as large as <NAME>’s blocksize.

1034 This mechanism has no parameters.

1035 Constraints on key types and the length of data are summarized in the following table:

1036 *Table 30, General Block Cipher MAC: Key and Data Length*

Function	Key type	Data length	Signature length
C_Sign	<NAME>	Any	[blocksize/2]
C_Verify	<NAME>	Any	[blocksize/2]

1037 For this mechanism, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO** structure  
1038 may or may not be used. The CAST, CAST3, and CAST128 (CAST5) ciphers have variable key sizes,  
1039 and so for these ciphers, the *ulMinKeySize* and *ulMaxKeySize* fields of the **CK\_MECHANISM\_INFO**  
1040 structure specify the supported range of key sizes, in bytes. For the DES, DES3 (triple-DES), IDEA and  
1041 CDMF ciphers, these fields are not used.



## 1042 2.7 SKIPJACK

### 1043 2.7.1 Definitions

1044 This section defines the key type “CKK\_SKIPJACK” for type CK\_KEY\_TYPE as used in the  
1045 CKA\_KEY\_TYPE attribute of key objects.

1046 Mechanisms:

- 1047 CKM\_SKIPJACK\_KEY\_GEN
- 1048 CKM\_SKIPJACK\_ECB64
- 1049 CKM\_SKIPJACK\_CBC64
- 1050 CKM\_SKIPJACK\_OFB64
- 1051 CKM\_SKIPJACK\_CFB64
- 1052 CKM\_SKIPJACK\_CFB32
- 1053 CKM\_SKIPJACK\_CFB16
- 1054 CKM\_SKIPJACK\_CFB8
- 1055 CKM\_SKIPJACK\_WRAP
- 1056 CKM\_SKIPJACK\_PRIVATE\_WRAP
- 1057 CKM\_SKIPJACK\_RELAYX

### 1058 2.7.2 SKIPJACK secret key objects

1059 SKIPJACK secret key objects (object class **CKO\_SECRET\_KEY**, key type **CKK\_SKIPJACK**) holds a  
1060 single-length MEK or a TEK. The following table defines the SKIPJACK secret object attributes, in  
1061 addition to the common attributes defined for this object class:

1062 *Table 31, SKIPJACK Secret Key Object*

Attribute	Data type	Meaning
CKA_VALUE <sup>1,4,6,7</sup>	Byte array	Key value (always 12 bytes long)

1063 Refer to [PKCS #11-Base] table 15 for footnotes

1064

1065 SKIPJACK keys have 16 checksum bits, and these bits must be properly set. Attempting to create or  
1066 unwrap a SKIPJACK key with incorrect checksum bits will return an error.

1067 It is not clear that any tokens exist (or ever will exist) which permit an application to create a SKIPJACK  
1068 key with a specified value. Nonetheless, we provide templates for doing so.

1069 The following is a sample template for creating a SKIPJACK MEK secret key object:

```
1070 CK_OBJECT_CLASS class = CKO_SECRET_KEY;  
1071 CK_KEY_TYPE keyType = CKK_SKIPJACK;  
1072 CK_UTF8CHAR label[] = "A SKIPJACK MEK secret key object";  
1073 CK_BYTE value[12] = {...};  
1074 CK_BBOOL true = CK_TRUE;  
1075 CK_ATTRIBUTE template[] = {  
1076     {CKA_CLASS, &class, sizeof(class)},  
1077     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},  
1078     {CKA_TOKEN, &true, sizeof(true)},  
1079     {CKA_LABEL, label, sizeof(label)-1},  
1080     {CKA_ENCRYPT, &true, sizeof(true)},  
1081     {CKA_VALUE, value, sizeof(value)}  
1082 };
```

1083 The following is a sample template for creating a SKIPJACK TEK secret key object:

```

1084 CK_OBJECT_CLASS class = CKO_SECRET_KEY;
1085 CK_KEY_TYPE keyType = CKK_SKIPJACK;
1086 CK_UTF8CHAR label[] = "A SKIPJACK TEK secret key object";
1087 CK_BYTE value[12] = {...};
1088 CK_BBOOL true = CK_TRUE;
1089 CK_ATTRIBUTE template[] = {
1090     {CKA_CLASS, &class, sizeof(class)},
1091     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},
1092     {CKA_TOKEN, &>true, sizeof(true)},
1093     {CKA_LABEL, label, sizeof(label)-1},
1094     {CKA_ENCRYPT, &>true, sizeof(true)},
1095     {CKA_WRAP, &>true, sizeof(true)},
1096     {CKA_VALUE, value, sizeof(value)}
1097 };

```

## 1098 2.7.3 SKIPJACK Mechanism parameters

### 1099 2.7.3.1 CK\_SKIPJACK\_PRIVATE\_WRAP\_PARAMS; 1100 CK\_SKIPJACK\_PRIVATE\_WRAP\_PARAMS\_PTR

1101 **CK\_SKIPJACK\_PRIVATE\_WRAP\_PARAMS** is a structure that provides the parameters to the  
1102 **CKM\_SKIPJACK\_PRIVATE\_WRAP** mechanism. It is defined as follows:

```

1103 typedef struct CK_SKIPJACK_PRIVATE_WRAP_PARAMS {
1104     CK_ULONG ulPasswordLen;
1105     CK_BYTE_PTR pPassword;
1106     CK_ULONG ulPublicDataLen;
1107     CK_BYTE_PTR pPublicData;
1108     CK_ULONG ulPandGLen;
1109     CK_ULONG ulQLen;
1110     CK_ULONG ulRandomLen;
1111     CK_BYTE_PTR pRandomA;
1112     CK_BYTE_PTR pPrimeP;
1113     CK_BYTE_PTR pBaseG;
1114     CK_BYTE_PTR pSubprimeQ;
1115 } CK_SKIPJACK_PRIVATE_WRAP_PARAMS;

```

1116 The fields of the structure have the following meanings:

1117	<i>ulPasswordLen</i>	length of the password
1118	<i>pPassword</i>	pointer to the buffer which contains the user-supplied password
1119		
1120	<i>ulPublicDataLen</i>	other party's key exchange public key size
1121	<i>pPublicData</i>	pointer to other party's key exchange public key value
1122	<i>ulPandGLen</i>	length of prime and base values
1123	<i>ulQLen</i>	length of subprime value
1124	<i>ulRandomLen</i>	size of random Ra, in bytes
1125	<i>pPrimeP</i>	pointer to Prime, p, value
1126	<i>pBaseG</i>	pointer to Base, b, value



1127 *pSubprimeQ* pointer to Subprime, q, value

1128 **CK\_SKIPJACK\_PRIVATE\_WRAP\_PARAMS\_PTR** is a pointer to a  
1129 **CK\_PRIVATE\_WRAP\_PARAMS**.

### 1130 **2.7.3.2 CK\_SKIPJACK\_RELAYX\_PARAMS;** 1131 **CK\_SKIPJACK\_RELAYX\_PARAMS\_PTR**

1132 **CK\_SKIPJACK\_RELAYX\_PARAMS** is a structure that provides the parameters to the  
1133 **CKM\_SKIPJACK\_RELAYX** mechanism. It is defined as follows:

```
1134 typedef struct CK_SKIPJACK_RELAYX_PARAMS {  
1135     CK_ULONG ulOldWrappedXLen;  
1136     CK_BYTE_PTR pOldWrappedX;  
1137     CK_ULONG ulOldPasswordLen;  
1138     CK_BYTE_PTR pOldPassword;  
1139     CK_ULONG ulOldPublicDataLen;  
1140     CK_BYTE_PTR pOldPublicData;  
1141     CK_ULONG ulOldRandomLen;  
1142     CK_BYTE_PTR pOldRandomA;  
1143     CK_ULONG ulNewPasswordLen;  
1144     CK_BYTE_PTR pNewPassword;  
1145     CK_ULONG ulNewPublicDataLen;  
1146     CK_BYTE_PTR pNewPublicData;  
1147     CK_ULONG ulNewRandomLen;  
1148     CK_BYTE_PTR pNewRandomA;  
1149 } CK_SKIPJACK_RELAYX_PARAMS;
```

1150 The fields of the structure have the following meanings:

1151 *ulOldWrappedLen* length of old wrapped key in bytes

1152 *pOldWrappedX* pointer to old wrapper key

1153 *ulOldPasswordLen* length of the old password

1154 *pOldPassword* pointer to the buffer which contains the old user-supplied  
1155 password

1156 *ulOldPublicDataLen* old key exchange public key size

1157 *pOldPublicData* pointer to old key exchange public key value

1158 *ulOldRandomLen* size of old random Ra in bytes

1159 *pOldRandomA* pointer to old Ra data

1160 *ulNewPasswordLen* length of the new password

1161 *pNewPassword* pointer to the buffer which contains the new user-  
1162 supplied password

1163 *ulNewPublicDataLen* new key exchange public key size

1164 *pNewPublicData* pointer to new key exchange public key value

1165 *ulNewRandomLen* size of new random Ra in bytes

1166 *pNewRandomA* pointer to new Ra data

1167 **CK\_SKIPJACK\_RELAYX\_PARAMS\_PTR** is a pointer to a **CK\_SKIPJACK\_RELAYX\_PARAMS**.

## 1168 2.7.4 SKIPJACK key generation

1169 The SKIPJACK key generation mechanism, denoted **CKM\_SKIPJACK\_KEY\_GEN**, is a key generation  
1170 mechanism for SKIPJACK. The output of this mechanism is called a Message Encryption Key (MEK).

1171 It does not have a parameter.

1172 The mechanism contributes the **CKA\_CLASS**, **CKA\_KEY\_TYPE**, and **CKA\_VALUE** attributes to the new  
1173 key.

## 1174 2.7.5 SKIPJACK-ECB64

1175 SKIPJACK-ECB64, denoted **CKM\_SKIPJACK\_ECB64**, is a mechanism for single- and multiple-part  
1176 encryption and decryption with SKIPJACK in 64-bit electronic codebook mode as defined in FIPS PUB  
1177 185.

1178 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
1179 value generated by the token – in other words, the application can't specify a particular IV when  
1180 encrypting. It can, of course, specify a particular IV when decrypting.

1181 Constraints on key types and the length of data are summarized in the following table:

1182 *Table 32, SKIPJACK-ECB64: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	SKIPJACK	Multiple of 8	Same as input length	No final part
C_Decrypt	SKIPJACK	Multiple of 8	Same as input length	No final part

## 1183 2.7.6 SKIPJACK-CBC64

1184 SKIPJACK-CBC64, denoted **CKM\_SKIPJACK\_CBC64**, is a mechanism for single- and multiple-part  
1185 encryption and decryption with SKIPJACK in 64-bit output feedback mode as defined in FIPS PUB 185.

1186 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
1187 value generated by the token – in other words, the application cannot specify a particular IV when  
1188 encrypting. It can, of course, specify a particular IV when decrypting.

1189 Constraints on key types and the length of data are summarized in the following table:

1190 *Table 33, SKIPJACK-CBC64: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	SKIPJACK	Multiple of 8	Same as input length	No final part
C_Decrypt	SKIPJACK	Multiple of 8	Same as input length	No final part

## 1191 2.7.7 SKIPJACK-OFB64

1192 SKIPJACK-OFB64, denoted **CKM\_SKIPJACK\_OFB64**, is a mechanism for single- and multiple-part  
1193 encryption and decryption with SKIPJACK in 64-bit output feedback mode as defined in FIPS PUB 185.

1194 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
1195 value generated by the token – in other words, the application cannot specify a particular IV when  
1196 encrypting. It can, of course, specify a particular IV when decrypting.

1197 Constraints on key types and the length of data are summarized in the following table:

1198 *Table 34, SKIPJACK-OFB64: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	SKIPJACK	Multiple of 8	Same as input length	No final part
C_Decrypt	SKIPJACK	Multiple of 8	Same as input length	No final part

## 1199 2.7.8 SKIPJACK-CFB64

1200 SKIPJACK-CFB64, denoted **CKM\_SKIPJACK\_CFB64**, is a mechanism for single- and multiple-part  
1201 encryption and decryption with SKIPJACK in 64-bit cipher feedback mode as defined in FIPS PUB 185.

1202 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
1203 value generated by the token – in other words, the application cannot specify a particular IV when  
1204 encrypting. It can, of course, specify a particular IV when decrypting.

1205 Constraints on key types and the length of data are summarized in the following table:

1206 *Table 35, SKIPJACK-CFB64: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	SKIPJACK	Multiple of 8	Same as input length	No final part
C_Decrypt	SKIPJACK	Multiple of 8	Same as input length	No final part

## 1207 2.7.9 SKIPJACK-CFB32

1208 SKIPJACK-CFB32, denoted **CKM\_SKIPJACK\_CFB32**, is a mechanism for single- and multiple-part  
1209 encryption and decryption with SKIPJACK in 32-bit cipher feedback mode as defined in FIPS PUB 185.

1210 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
1211 value generated by the token – in other words, the application cannot specify a particular IV when  
1212 encrypting. It can, of course, specify a particular IV when decrypting.

1213 Constraints on key types and the length of data are summarized in the following table:

1214 *Table 36, SKIPJACK-CFB32: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	SKIPJACK	Multiple of 4	Same as input length	No final part
C_Decrypt	SKIPJACK	Multiple of 4	Same as input length	No final part

## 1215 2.7.10 SKIPJACK-CFB16

1216 SKIPJACK-CFB16, denoted **CKM\_SKIPJACK\_CFB16**, is a mechanism for single- and multiple-part  
1217 encryption and decryption with SKIPJACK in 16-bit cipher feedback mode as defined in FIPS PUB 185.

1218 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
1219 value generated by the token – in other words, the application cannot specify a particular IV when  
1220 encrypting. It can, of course, specify a particular IV when decrypting.

1221 Constraints on key types and the length of data are summarized in the following table:

1222 *Table 37, SKIPJACK-CFB16: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	SKIPJACK	Multiple of 4	Same as input length	No final part

C_Decrypt	SKIPJACK	Multiple of 4	Same as input length	No final part
-----------	----------	---------------	----------------------	---------------

### 1223 2.7.11 SKIPJACK-CFB8

1224 SKIPJACK-CFB8, denoted **CKM\_SKIPJACK\_CFB8**, is a mechanism for single- and multiple-part  
1225 encryption and decryption with SKIPJACK in 8-bit cipher feedback mode as defined in FIPS PUB 185.

1226 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
1227 value generated by the token – in other words, the application cannot specify a particular IV when  
1228 encrypting. It can, of course, specify a particular IV when decrypting.

1229 Constraints on key types and the length of data are summarized in the following table:

1230 *Table 38, SKIPJACK-CFB8: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	SKIPJACK	Multiple of 4	Same as input length	No final part
C_Decrypt	SKIPJACK	Multiple of 4	Same as input length	No final part

### 1231 2.7.12 SKIPJACK-WRAP

1232 The SKIPJACK-WRAP mechanism, denoted **CKM\_SKIPJACK\_WRAP**, is used to wrap and unwrap a  
1233 secret key (MEK). It can wrap or unwrap SKIPJACK, BATON, and JUNIPER keys.

1234 It does not have a parameter.

### 1235 2.7.13 SKIPJACK-PRIVATE-WRAP

1236 The SKIPJACK-PRIVATE-WRAP mechanism, denoted **CKM\_SKIPJACK\_PRIVATE\_WRAP**, is used to  
1237 wrap and unwrap a private key. It can wrap KEA and DSA private keys.

1238 It has a parameter, a **CK\_SKIPJACK\_PRIVATE\_WRAP\_PARAMS** structure.

### 1239 2.7.14 SKIPJACK-RELAYX

1240 The SKIPJACK-RELAYX mechanism, denoted **CKM\_SKIPJACK\_RELAYX**, is used with the **C\_WrapKey**  
1241 function to “change the wrapping” on a private key which was wrapped with the SKIPJACK-PRIVATE-  
1242 WRAP mechanism (See Section 2.7.13).

1243 It has a parameter, a **CK\_SKIPJACK\_RELAYX\_PARAMS** structure.

1244 Although the SKIPJACK-RELAYX mechanism is used with **C\_WrapKey**, it differs from other key-  
1245 wrapping mechanisms. Other key-wrapping mechanisms take a key handle as one of the arguments to  
1246 **C\_WrapKey**; however for the SKIPJACK\_RELAYX mechanism, the [always invalid] value 0 should be  
1247 passed as the key handle for **C\_WrapKey**, and the already-wrapped key should be passed in as part of  
1248 the **CK\_SKIPJACK\_RELAYX\_PARAMS** structure.

## 1249 2.8 BATON

### 1250 2.8.1 Definitions

1251 This section defines the key type “CKK\_BATON” for type CK\_KEY\_TYPE as used in the  
1252 CKA\_KEY\_TYPE attribute of key objects.

1253 Mechanisms:

1254 CKM\_BATON\_KEY\_GEN

1255 CKM\_BATON\_ECB128

1256 CKM\_BATON\_ECB96

1257 CKM\_BATON\_CBC128  
1258 CKM\_BATON\_COUNTER  
1259 CKM\_BATON\_SHUFFLE  
1260 CKM\_BATON\_WRAP

## 1261 2.8.2 BATON secret key objects

1262 BATON secret key objects (object class **CKO\_SECRET\_KEY**, key type **CKK\_BATON**) hold single-length  
1263 BATON keys. The following table defines the BATON secret key object attributes, in addition to the  
1264 common attributes defined for this object class:

1265 *Table 39, BATON Secret Key Object*

Attribute	Data type	Meaning
CKA_VALUE <sup>1,4,6,7</sup>	Byte array	Key value (always 40 bytes long)

1266 Refer to [PKCS #11-Base] table 15 for footnotes

1267

1268 BATON keys have 160 checksum bits, and these bits must be properly set. Attempting to create or  
1269 unwrap a BATON key with incorrect checksum bits will return an error.

1270 It is not clear that any tokens exist (or will ever exist) which permit an application to create a BATON key  
1271 with a specified value. Nonetheless, we provide templates for doing so.

1272 The following is a sample template for creating a BATON MEK secret key object:

```
1273 CK_OBJECT_CLASS class = CKO_SECRET_KEY;  
1274 CK_KEY_TYPE keyType = CKK_BATON;  
1275 CK_UTF8CHAR label[] = "A BATON MEK secret key object";  
1276 CK_BYTE value[40] = {...};  
1277 CK_BBOOL true = CK_TRUE;  
1278 CK_ATTRIBUTE template[] = {  
1279     {CKA_CLASS, &class, sizeof(class)},  
1280     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},  
1281     {CKA_TOKEN, &>true, sizeof(true)},  
1282     {CKA_LABEL, label, sizeof(label)-1},  
1283     {CKA_ENCRYPT, &>true, sizeof(true)},  
1284     {CKA_VALUE, value, sizeof(value)}  
1285 };
```

1286 The following is a sample template for creating a BATON TEK secret key object:

```
1287 CK_OBJECT_CLASS class = CKO_SECRET_KEY;  
1288 CK_KEY_TYPE keyType = CKK_BATON;  
1289 CK_UTF8CHAR label[] = "A BATON TEK secret key object";  
1290 CK_BYTE value[40] = {...};  
1291 CK_BBOOL true = CK_TRUE;  
1292 CK_ATTRIBUTE template[] = {  
1293     {CKA_CLASS, &class, sizeof(class)},  
1294     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},  
1295     {CKA_TOKEN, &>true, sizeof(true)},  
1296     {CKA_LABEL, label, sizeof(label)-1},  
1297     {CKA_ENCRYPT, &>true, sizeof(true)},  
1298     {CKA_WRAP, &>true, sizeof(true)},  
1299     {CKA_VALUE, value, sizeof(value)}  
1300 };
```

## 1301 2.8.3 BATON key generation

1302 The BATON key generation mechanism, denoted **CKM\_BATON\_KEY\_GEN**, is a key generation  
1303 mechanism for BATON. The output of this mechanism is called a Message Encryption Key (MEK).

1304 It does not have a parameter.  
 1305 The mechanism contributes the **CKA\_CLASS**, **CKA\_KEY\_TYPE**, and **CKA\_VALUE** attributes to the new  
 1306 key.

### 1307 **2.8.4 BATON-ECB128**

1308 BATON-ECB128, denoted **CKM\_BATON\_ECB128**, is a mechanism for single- and multiple-part  
 1309 encryption and decryption with BATON in 128-bit electronic codebook mode.  
 1310 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
 1311 value generated by the token – in other words, the application cannot specify a particular IV when  
 1312 encrypting. It can, of course, specify a particular IV when decrypting.  
 1313 Constraints on key types and the length of data are summarized in the following table:

1314 *Table 40, BATON-ECB128: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	BATON	Multiple of 16	Same as input length	No final part
C_Decrypt	BATON	Multiple of 16	Same as input length	No final part

### 1315 **2.8.5 BATON-ECB96**

1316 BATON-ECB96, denoted **CKM\_BATON\_ECB96**, is a mechanism for single- and multiple-part encryption  
 1317 and decryption with BATON in 96-bit electronic codebook mode.  
 1318 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
 1319 value generated by the token – in other words, the application cannot specify a particular IV when  
 1320 encrypting. It can, of course, specify a particular IV when decrypting.

1321 Constraints on key types and the length of data are summarized in the following table:

1322 *Table 41, BATON-ECB96: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	BATON	Multiple of 12	Same as input length	No final part
C_Decrypt	BATON	Multiple of 12	Same as input length	No final part

### 1323 **2.8.6 BATON-CBC128**

1324 BATON-CBC128, denoted **CKM\_BATON\_CBC128**, is a mechanism for single- and multiple-part  
 1325 encryption and decryption with BATON in 128-bit cipher-block chaining mode.  
 1326 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
 1327 value generated by the token – in other words, the application cannot specify a particular IV when  
 1328 encrypting. It can, of course, specify a particular IV when decrypting.

1329 Constraints on key types and the length of data are summarized in the following table:

1330 *Table 42, BATON-CBC128*

Function	Key type	Input length	Output length	Comments
C_Encrypt	BATON	Multiple of 16	Same as input length	No final part
C_Decrypt	BATON	Multiple of 16	Same as input length	No final part



## 1331 2.8.7 BATON-COUNTER

1332 BATON-COUNTER, denoted **CKM\_BATON\_COUNTER**, is a mechanism for single- and multiple-part  
1333 encryption and decryption with BATON in counter mode.

1334 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
1335 value generated by the token – in other words, the application cannot specify a particular IV when  
1336 encrypting. It can, of course, specify a particular IV when decrypting.

1337 Constraints on key types and the length of data are summarized in the following table:

1338 *Table 43, BATON-COUNTER: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	BATON	Multiple of 16	Same as input length	No final part
C_Decrypt	BATON	Multiple of 16	Same as input length	No final part

## 1339 2.8.8 BATON-SHUFFLE

1340 BATON-SHUFFLE, denoted **CKM\_BATON\_SHUFFLE**, is a mechanism for single- and multiple-part  
1341 encryption and decryption with BATON in shuffle mode.

1342 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
1343 value generated by the token – in other words, the application cannot specify a particular IV when  
1344 encrypting. It can, of course, specify a particular IV when decrypting.

1345 Constraints on key types and the length of data are summarized in the following table:

1346 *Table 44, BATON-SHUFFLE: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	BATON	Multiple of 16	Same as input length	No final part
C_Decrypt	BATON	Multiple of 16	Same as input length	No final part

## 1347 2.8.9 BATON WRAP

1348 The BATON wrap and unwrap mechanism, denoted **CKM\_BATON\_WRAP**, is a function used to wrap  
1349 and unwrap a secret key (MEK). It can wrap and unwrap SKIPJACK, BATON and JUNIPER keys.

1350 It has no parameters.

1351 When used to unwrap a key, this mechanism contributes the **CKA\_CLASS**, **CKA\_KEY\_TYPE**, and  
1352 **CKA\_VALUE** attributes to it.

## 1353 2.9 JUNIPER

### 1354 2.9.1 Definitions

1355 This section defines the key type “CKK\_JUNIPER” for type CK\_KEY\_TYPE as used in the  
1356 CKA\_KEY\_TYPE attribute of key objects.

1357 Mechanisms:

1358 CKM\_JUNIPER\_KEY\_GEN

1359 CKM\_JUNIPER\_ECB128

1360 CKM\_JUNIPER\_CBC128

1361 CKM\_JUNIPER\_COUNTER

1362 CKM\_JUNIPER\_SHUFFLE

1363 CKM\_JUNIPER\_WRAP

## 1364 2.9.2 JUNIPER secret key objects

1365 JUNIPER secret key objects (object class **CKO\_SECRET\_KEY**, key type **CKK\_JUNIPER**) hold single-  
1366 length JUNIPER keys. The following table defines the BATON secret key object attributes, in addition to  
1367 the common attributes defined for this object class:

1368 *Table 45, JUNIPER Secret Key Object*

Attribute	Data type	Meaning
CKA_VALUE <sup>1,4,6,7</sup>	Byte array	Key value (always 40 bytes long)

1369 Refer to [PKCS #11-Base] table 15 for footnotes

1370

1371 JUNIPER keys have 160 checksum bits, and these bits must be properly set. Attempting to create or  
1372 unwrap a BATON key with incorrect checksum bits will return an error.

1373 It is not clear that any tokens exist (or will ever exist) which permit an application to create a BATON key  
1374 with a specified value. Nonetheless, we provide templates for doing so.

1375 The following is a sample template for creating a JUNIPER MEK secret key object:

```
1376 CK_OBJECT_CLASS class = CKO_SECRET_KEY;  
1377 CK_KEY_TYPE keyType = CKK_JUNIPER;  
1378 CK_UTF8CHAR label[] = "A JUNIPER MEK secret key object";  
1379 CK_BYTE value[40] = {...};  
1380 CK_BBOOL true = CK_TRUE;  
1381 CK_ATTRIBUTE template[] = {  
1382     {CKA_CLASS, &class, sizeof(class)},  
1383     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},  
1384     {CKA_TOKEN, &>true, sizeof(true)},  
1385     {CKA_LABEL, label, sizeof(label)-1},  
1386     {CKA_ENCRYPT, &>true, sizeof(true)},  
1387     {CKA_VALUE, value, sizeof(value)}  
1388 };
```

1389 The following is a sample template for creating a JUNIPER TEK secret key object:

```
1390 CK_OBJECT_CLASS class = CKO_SECRET_KEY;  
1391 CK_KEY_TYPE keyType = CKK_JUNIPER;  
1392 CK_UTF8CHAR label[] = "A JUNIPER TEK secret key object";  
1393 CK_BYTE value[40] = {...};  
1394 CK_BBOOL true = CK_TRUE;  
1395 CK_ATTRIBUTE template[] = {  
1396     {CKA_CLASS, &class, sizeof(class)},  
1397     {CKA_KEY_TYPE, &keyType, sizeof(keyType)},  
1398     {CKA_TOKEN, &>true, sizeof(true)},  
1399     {CKA_LABEL, label, sizeof(label)-1},  
1400     {CKA_ENCRYPT, &>true, sizeof(true)},  
1401     {CKA_WRAP, &>true, sizeof(true)},  
1402     {CKA_VALUE, value, sizeof(value)}  
1403 };
```

## 1404 2.9.3 JUNIPER key generation

1405 The JUNIPER key generation mechanism, denoted **CKM\_JUNIPER\_KEY\_GEN**, is a key generation  
1406 mechanism for JUNIPER. The output of this mechanism is called a Message Encryption Key (MEK).

1407 It does not have a parameter.

1408 The mechanism contributes the **CKA\_CLASS**, **CKA\_KEY\_TYPE**, and **CKA\_VALUE** attributes to the new  
1409 key.



## 1410 2.9.4 JUNIPER-ECB128

1411 JUNIPER-ECB128, denoted **CKM\_JUNIPER\_ECB128**, is a mechanism for single- and multiple-part  
1412 encryption and decryption with JUNIPER in 128-bit electronic codebook mode.

1413 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
1414 value generated by the token – in other words, the application cannot specify a particular IV when  
1415 encrypting. It can, of course, specify a particular IV when decrypting.

1416 Constraints on key types and the length of data are summarized in the following table. For encryption  
1417 and decryption, the input and output data (parts) may begin at the same location in memory.

1418 *Table 46, JUNIPER-ECB128: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	JUNIPER	Multiple of 16	Same as input length	No final part
C_Decrypt	JUNIPER	Multiple of 16	Same as input length	No final part

## 1419 2.9.5 JUNIPER-CBC128

1420 JUNIPER-CBC128, denoted **CKM\_JUNIPER\_CBC128**, is a mechanism for single- and multiple-part  
1421 encryption and decryption with JUNIPER in 128-bit cipher block chaining mode.

1422 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
1423 value generated by the token – in other words, the application cannot specify a particular IV when  
1424 encrypting. It can, of course, specify a particular IV when decrypting.

1425 Constraints on key types and the length of data are summarized in the following table. For encryption  
1426 and decryption, the input and output data (parts) may begin at the same location in memory.

1427 *Table 47, JUNIPER-CBC128: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	JUNIPER	Multiple of 16	Same as input length	No final part
C_Decrypt	JUNIPER	Multiple of 16	Same as input length	No final part

## 1428 2.9.6 JUNIPER-COUNTER

1429 JUNIPER-COUNTER, denoted **CKM\_JUNIPER\_COUNTER**, is a mechanism for single- and multiple-  
1430 part encryption and decryption with JUNIPER in counter mode.

1431 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
1432 value generated by the token – in other words, the application cannot specify a particular IV when  
1433 encrypting. It can, of course, specify a particular IV when decrypting.

1434 Constraints on key types and the length of data are summarized in the following table. For encryption  
1435 and decryption, the input and output data (parts) may begin at the same location in memory.

1436 *Table 48, JUNIPER-COUNTER: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	JUNIPER	Multiple of 16	Same as input length	No final part
C_Decrypt	JUNIPER	Multiple of 16	Same as input length	No final part

## 1437 2.9.7 JUNIPER-SHUFFLE

1438 JUNIPER-SHUFFLE, denoted **CKM\_JUNIPER\_SHUFFLE**, is a mechanism for single- and multiple-part  
1439 encryption and decryption with JUNIPER in shuffle mode.

1440 It has a parameter, a 24-byte initialization vector. During an encryption operation, this IV is set to some  
1441 value generated by the token – in other words, the application cannot specify a particular IV when  
1442 encrypting. It can, of course, specify a particular IV when decrypting.

1443 Constraints on key types and the length of data are summarized in the following table. For encryption  
1444 and decryption, the input and output data (parts) may begin at the same location in memory.

1445 *Table 49, JUNIPER-SHUFFLE: Data and Length*

Function	Key type	Input length	Output length	Comments
C_Encrypt	JUNIPER	Multiple of 16	Same as input length	No final part
C_Decrypt	JUNIPER	Multiple of 16	Same as input length	No final part

## 1446 2.9.8 JUNIPER WRAP

1447 The JUNIPER wrap and unwrap mechanism, denoted **CKM\_JUNIPER\_WRAP**, is a function used to wrap  
1448 and unwrap an MEK. It can wrap or unwrap SKIPJACK, BATON and JUNIPER keys.

1449 It has no parameters.

1450 When used to unwrap a key, this mechanism contributes the **CKA\_CLASS**, **CKA\_KEY\_TYPE**, and  
1451 **CKA\_VALUE** attributes to it.

## 1452 2.10 MD2

### 1453 2.10.1 Definitions

1454 Mechanisms:

1455 CKM\_MD2

1456 CKM\_MD2\_HMAC

1457 CKM\_MD2\_HMAC\_GENERAL

1458 CKM\_MD2\_KEY\_DERIVATION

### 1459 2.10.2 MD2 digest

1460 The MD2 mechanism, denoted **CKM\_MD2**, is a mechanism for message digesting, following the MD2  
1461 message-digest algorithm defined in RFC 1319.

1462 It does not have a parameter.

1463 Constraints on the length of data are summarized in the following table:

1464 *Table 50, MD2: Data Length*

Function	Data length	Digest Length
C_Digest	Any	16

### 1465 2.10.3 General-length MD2-HMAC

1466 The general-length MD2-HMAC mechanism, denoted **CKM\_MD2\_HMAC\_GENERAL**, is a mechanism for  
1467 signatures and verification. It uses the HMAC construction, based on the MD2 hash function. The keys it  
1468 uses are generic secret keys.

1469 It has a parameter, a **CK\_MAC\_GENERAL\_PARAMS**, which holds the length in bytes of the desired  
1470 output. This length should be in the range 0-16 (the output size of MD2 is 16 bytes). Signatures (MACs)  
1471 produced by this mechanism will be taken from the start of the full 16-byte HMAC output.

1472 Table 51, General-length MD2-HMAC: Key and Data Length

Function	Key type	Data length	Signature length
C_Sign	Generic secret	Any	0-16, depending on parameters
C_Verify	Generic secret	Any	0-16, depending on parameters

## 1473 2.10.4 MD2-HMAC

1474 The MD2-HMAC mechanism, denoted **CKM\_MD2\_HMAC**, is a special case of the general-length MD2-  
1475 HMAC mechanism in Section 2.10.3.

1476 It has no parameter, and always produces an output of length 16.

## 1477 2.10.5 MD2 key derivation

1478 MD2 key derivation, denoted **CKM\_MD2\_KEY\_DERIVATION**, is a mechanism which provides the  
1479 capability of deriving a secret key by digesting the value of another secret key with MD2.

1480 The value of the base key is digested once, and the result is used to make the value of the derived secret  
1481 key.

- 1482 • If no length or key type is provided in the template, then the key produced by this mechanism will be a  
1483 generic secret key. Its length will be 16 bytes (the output size of MD2)..
- 1484 • If no key type is provided in the template, but a length is, then the key produced by this mechanism  
1485 will be a generic secret key of the specified length.
- 1486 • If no length was provided in the template, but a key type is, then that key type must have a well-  
1487 defined length. If it does, then the key produced by this mechanism will be of the type specified in the  
1488 template. If it doesn't, an error will be returned.
- 1489 • If both a key type and a length are provided in the template, the length must be compatible with that  
1490 key type. The key produced by this mechanism will be of the specified type and length.

1491 If a DES, DES2, or CDMF key is derived with this mechanism, the parity bits of the key will be set  
1492 properly.

1493 If the requested type of key requires more than 16 bytes, such as DES2, an error is generated.

1494 This mechanism has the following rules about key sensitivity and extractability:

- 1495 • The **CKA\_SENSITIVE** and **CKA\_EXTRACTABLE** attributes in the template for the new key can both  
1496 be specified to be either CK\_TRUE or CK\_FALSE. If omitted, these attributes each take on some  
1497 default value.
- 1498 • If the base key has its **CKA\_ALWAYS\_SENSITIVE** attribute set to CK\_FALSE, then the derived key  
1499 will as well. If the base key has its **CKA\_ALWAYS\_SENSITIVE** attribute set to CK\_TRUE, then the  
1500 derived key has its **CKA\_ALWAYS\_SENSITIVE** attribute set to the same value as its  
1501 **CKA\_SENSITIVE** attribute.
- 1502 • Similarly, if the base key has its **CKA\_NEVER\_EXTRACTABLE** attribute set to CK\_FALSE, then the  
1503 derived key will, too. If the base key has its **CKA\_NEVER\_EXTRACTABLE** attribute set to  
1504 CK\_TRUE, then the derived key has its **CKA\_NEVER\_EXTRACTABLE** attribute set to the *opposite*  
1505 value from its **CKA\_EXTRACTABLE** attribute.

## 1506 2.11 MD5

### 1507 2.11.1 Definitions

1508 Mechanisms:

1509 CKM\_MD5

1510 CKM\_MD5\_HMAC

1511 CKM\_MD5\_HMAC\_GENERAL  
1512 CKM\_MD5\_KEY\_DERIVATION

### 1513 2.11.2 MD5 Digest

1514 The MD5 mechanism, denoted **CKM\_MD5**, is a mechanism for message digesting, following the MD5  
1515 message-digest algorithm defined in RFC 1321.

1516 It does not have a parameter.

1517 Constraints on the length of input and output data are summarized in the following table. For single-part  
1518 digesting, the data and the digest may begin at the same location in memory.

1519 *Table 52, MD5: Data Length*

Function	Data length	Digest length
C_Digest	Any	16

### 1520 2.11.3 General-length MD5-HMAC

1521 The general-length MD5-HMAC mechanism, denoted **CKM\_MD5\_HMAC\_GENERAL**, is a mechanism for  
1522 signatures and verification. It uses the HMAC construction, based on the MD5 hash function. The keys it  
1523 uses are generic secret keys.

1524 It has a parameter, a **CK\_MAC\_GENERAL\_PARAMS**, which holds the length in bytes of the desired  
1525 output. This length should be in the range 0-16 (the output size of MD5 is 16 bytes). Signatures (MACs)  
1526 produced by this mechanism will be taken from the start of the full 16-byte HMAC output.

1527 *Table 53, General-length MD5-HMAC: Key and Data Length*

Function	Key type	Data length	Signature length
C_Sign	Generic secret	Any	0-16, depending on parameters
C_Verify	Generic secret	Any	0-16, depending on parameters

### 1528 2.11.4 MD5-HMAC

1529 The MD5-HMAC mechanism, denoted **CKM\_MD5\_HMAC**, is a special case of the general-length MD5-  
1530 HMAC mechanism in Section 2.11.3.

1531 It has no parameter, and always produces an output of length 16.

### 1532 2.11.5 MD5 key derivation

1533 MD5 key derivation denoted **CKM\_MD5\_KEY\_DERIVATION**, is a mechanism which provides the  
1534 capability of deriving a secret key by digesting the value of another secret key with MD5.

1535 The value of the base key is digested once, and the result is used to make the value of derived secret  
1536 key.

- 1537
- 1538 • If no length or key type is provided in the template, then the key produced by this mechanism will be a generic secret key. Its length will be 16 bytes (the output size of MD5).
  - 1539 • If no key type is provided in the template, but a length is, then the key produced by this mechanism  
1540 will be a generic secret key of the specified length.
  - 1541 • If no length was provided in the template, but a key type is, then that key type must have a well-  
1542 defined length. If it does, then the key produced by this mechanism will be of the type specified in the  
1543 template. If it doesn't, an error will be returned.
  - 1544 • If both a key type and a length are provided in the template, the length must be compatible with that  
1545 key type. The key produced by this mechanism will be of the specified type and length.

1546 If a DES, DES2, or CDMF key is derived with this mechanism, the parity bits of the key will be set  
 1547 properly.

1548 If the requested type of key requires more than 16 bytes, such as DES3, an error is generated.

1549 This mechanism has the following rules about key sensitivity and extractability.

- 1550 • The **CKA\_SENSITIVE** and **CKA\_EXTRACTABLE** attributes in the template for the new key can both  
 1551 be specified to either CK\_TRUE or CK\_FALSE. If omitted, these attributes each take on some  
 1552 default value.
- 1553 • If the base key has its **CKA\_ALWAYS\_SENSITIVE** attribute set to CK\_FALSE, then the derived key  
 1554 will as well. If the base key has its **CKA\_ALWAYS\_SENSITIVE** attribute set to CK\_TRUE, then the  
 1555 derived key has its **CKA\_ALWAYS\_SENSITIVE** attribute set to the same value as its  
 1556 **CKA\_SENSITIVE** attribute.
- 1557 • Similarly, if the base key has its **CKA\_NEVER\_EXTRACTABLE** attribute set to CK\_FALSE, then the  
 1558 derived key will, too. If the base key has its **CKA\_NEVER\_EXTRACTABLE** attribute set to  
 1559 CK\_TRUE, then the derived key has its **CKA\_NEVER\_EXTRACTABLE** attribute set to the *opposite*  
 1560 value from its **CKA\_EXTRACTABLE** attribute.

## 1561 2.12 FASTHASH

### 1562 2.12.1 Definitions

1563 Mechanisms:  
 1564 CKM\_FASTHASH

### 1565 2.12.2 FASTHASH digest

1566 The FASTHASH mechanism, denoted **CKM\_FASTHASH**, is a mechanism for message digesting,  
 1567 following the U.S. government's algorithm.

1568 It does not have a parameter.

1569 Constraints on the length of input and output data are summarized in the following table:

1570 *Table 54, FASTHASH: Data Length*

Function	Input length	Digest length
C_Digest	Any	40

## 1571 2.13 PKCS #5 and PKCS #5-style password-based encryption (PBD)

1572 The mechanisms in this section are for generating keys and IVs for performing password-based  
 1573 encryption. The method used to generate keys and IVs is specified in PKCS #5.

### 1574 2.13.1 Definitions

1575 Mechanisms:

- 1576 CKM\_PBE\_MD2\_DES\_CBC
- 1577 CKM\_PBE\_MD5\_DES\_CBC
- 1578 CKM\_PBE\_MD5\_CAST\_CBC
- 1579 CKM\_PBE\_MD5\_CAST3\_CBC
- 1580 CKM\_PBE\_MD5\_CAST5\_CBC
- 1581 CKM\_PBE\_MD5\_CAST128\_CBC
- 1582 CKM\_PBE\_SHA1\_CAST5\_CBC
- 1583 CKM\_PBE\_SHA1\_CAST128\_CBC

1584 CKM\_PBE\_SHA1\_RC4\_128  
1585 CKM\_PBE\_SHA1\_RC4\_40  
1586 CKM\_PBE\_SHA1\_RC2\_128\_CBC  
1587 CKM\_PBE\_SHA1\_RC2\_40\_CBC

## 1588 2.13.2 Password-based encryption/authentication mechanism parameters

### 1589 2.13.2.1 CK\_PBE\_PARAMS; CK\_PBE\_PARAMS\_PTR

1590 **CK\_PBE\_PARAMS** is a structure which provides all of the necessary information required by the  
1591 CKM\_PBE mechanisms (see PKCS #5 and PKCS #12 for information on the PBE generation  
1592 mechanisms) and the CKM\_PBA\_SHA1\_WITH\_SHA1\_HMAC mechanism. It is defined as follows:

```
1593 typedef struct CK_PBE_PARAMS {  
1594     CK_BYTE_PTR pInitVector;  
1595     CK_UTF8CHAR_PTR pPassword;  
1596     CK_ULONG ulPasswordLen;  
1597     CK_BYTE_PTR pSalt;  
1598     CK_ULONG ulSaltLen;  
1599     CK_ULONG ulIteration;  
1600 } CK_PBE_PARAMS;
```

1601 The fields of the structure have the following meanings:

1602	<i>pInitVector</i>	pointer to the location that receives the 8-byte 1603 initialization vector (IV), if an IV is required
1604	<i>pPassword</i>	points to the password to be used in the PBE key 1605 generation
1606	<i>ulPasswordLen</i>	length in bytes of the password information
1607	<i>pSalt</i>	points to the salt to be used in the PBE key generation
1608	<i>ulSaltLen</i>	length in bytes of the salt information
1609	<i>ulliteration</i>	number of iterations required for the generation

1610 **CK\_PBE\_PARAMS\_PTR** is a pointer to a **CK\_PBE\_PARAMS**.

### 1611 2.13.3 MD2-PBE for DES-CBC

1612 MD2-PBE for DES-CBC, denoted **CKM\_PBE\_MD2\_DES\_CBC**, is a mechanism used for generating a  
1613 DES secret key and an IV from a password and a salt value by using the MD2 digest algorithm and an  
1614 iteration count. This functionality is defined in PKCS #5 as PBKDF1.

1615 It has a parameter, a **CK\_PBE\_PARAMS** structure. The parameter specifies the input information for the  
1616 key generation process and the location of the application-supplied buffer which will receive the 8-byte IV  
1617 generated by the mechanism.

### 1618 2.13.4 MD5-PBE for DES-CBC

1619 MD5-PBE for DES-CBC, denoted **CKM\_PBE\_MD5\_DES\_CBC**, is a mechanism used for generating a  
1620 DES secret key and an IV from a password and a salt value by using the MD5 digest algorithm and an  
1621 iteration count. This functionality is defined in PKCS #5 as PBKDF1.



1622 It has a parameter, a **CK\_PBE\_PARAMS** structure. The parameter specifies the input information for the  
1623 key generation process and the location of the application-supplied buffer which will receive the 8-byte IV  
1624 generated by the mechanism.

### 1625 **2.13.5 MD5-PBE for CAST-CBC**

1626 MD5-PBE for CAST-CBC, denoted **CKM\_PBE\_MD5\_CAST\_CBC**, is a mechanism used for generating a  
1627 CAST secret key and an IV from a password and a salt value by using the MD5 digest algorithm and an  
1628 iteration count. This functionality is analogous to that defined in PKCS #5 PBKDF1 for MD5 and DES.

1629 It has a parameter, a **CK\_PBE\_PARAMS** structure. The parameter specifies the input information for the  
1630 key generation process and the location of the application-supplied buffer which will receive the 8-byte IV  
1631 generated by the mechanism

1632 The length of the CAST key generated by this mechanism may be specified in the supplied template; if it  
1633 is not present in the template, it defaults to 8 bytes.

### 1634 **2.13.6 MD5-PBE for CAST3-CBC**

1635 MD5-PBE for CAST3-CBC, denoted **CKM\_PBE\_MD5\_CAST3\_CBC**, is a mechanism used for generating  
1636 a CAST3 secret key and an IV from a password and a salt value by using the MD5 digest algorithm and  
1637 an iteration count. This functionality is analogous to that defined in PKCS #5 PBKDF1 for MD5 and DES.

1638 It has a parameter, a **CK\_PBE\_PARAMS** structure. The parameter specifies the input information for the  
1639 key generation process and the location of the application-supplied buffer which will receive the 8-byte IV  
1640 generated by the mechanism

1641 The length of the CAST3 key generated by this mechanism may be specified in the supplied template; if it  
1642 is not present in the template, it defaults to 8 bytes.

### 1643 **2.13.7 MD5-PBE for CAST128-CBC (CAST5-CBC)**

1644 MD5-PBE for CAST128-CBC (CAST5-CBC), denoted **CKM\_PBE\_MD5\_CAST128\_CBC** or  
1645 **CKM\_PBE\_MD5\_CAST5\_CBC**, is a mechanism used for generating a CAST128 (CAST5) secret key  
1646 and an IV from a password and a salt value by using the MD5 digest algorithm and an iteration count.  
1647 This functionality is analogous to that defined in PKCS #5 PBKDF1 for MD5 and DES.

1648 It has a parameter, a **CK\_PBE\_PARAMS** structure. The parameter specifies the input information for the  
1649 key generation process and the location of the application-supplied buffer which will receive the 8-byte IV  
1650 generated by the mechanism

1651 The length of the CAST128 (CAST5) key generated by this mechanism may be specified in the supplied  
1652 template; if it is not present in the template, it defaults to 8 bytes.

### 1653 **2.13.8 SHA-1-PBE for CAST128-CBC (CAST5-CBC)**

1654 SHA-1-PBE for CAST128-CBC (CAST5-CBC), denoted **CKM\_PBE\_SHA1\_CAST128\_CBC** or  
1655 **CKM\_PBE\_SHA1\_CAST5\_CBC**, is a mechanism used for generating a CAST128 (CAST5) secret key  
1656 and an IV from a password and salt value using the SHA-1 digest algorithm and an iteration count. This  
1657 functionality is analogous to that defined in PKCS #5 PBKDF1 for MD5 and DES.

1658 It has a parameter, a **CK\_PBE\_PARAMS** structure. The parameter specifies the input information for the  
1659 key generation process and the location of the application-supplied buffer which will receive the 8-byte IV  
1660 generated by the mechanism

1661 The length of the CAST128 (CAST5) key generated by this mechanism may be specified in the supplied  
1662 template; if it is not present in the template, it defaults to 8 bytes



## 1663 2.14 PKCS #12 password-based encryption/authentication 1664 mechanisms

1665 The mechanisms in this section are for generating keys and IVs for performing password-based  
1666 encryption or authentication. The method used to generate keys and IVs is based on a method that was  
1667 specified in PKCS #12.

1668 We specify here a general method for producing various types of pseudo-random bits from a password,  
1669  $p$ ; a string of salt bits,  $s$ ; and an iteration count,  $c$ . The “type” of pseudo-random bits to be produced is  
1670 identified by an identification byte,  $ID$ , the meaning of which will be discussed later.

1671 Let  $H$  be a hash function built around a compression function  $f: \mathbf{Z}_2^u \times \mathbf{Z}_2^v \rightarrow \mathbf{Z}_2^u$  (that is,  $H$  has a chaining  
1672 variable and output of length  $u$  bits, and the message input to the compression function of  $H$  is  $v$  bits). For  
1673 MD2 and MD5,  $u=128$  and  $v=512$ ; for SHA-1,  $u=160$  and  $v=512$ .

1674 We assume here that  $u$  and  $v$  are both multiples of 8, as are the lengths in bits of the password and salt  
1675 strings and the number  $n$  of pseudo-random bits required. In addition,  $u$  and  $v$  are of course nonzero.

- 1676 1. Construct a string,  $D$  (the “diversifier”), by concatenating  $v/8$  copies of  $ID$ .
- 1677 2. Concatenate copies of the salt together to create a string  $S$  of length  $v \cdot \lceil s/v \rceil$  bits (the final copy of  
1678 the salt may be truncated to create  $S$ ). Note that if the salt is the empty string, then so is  $S$ .
- 1679 3. Concatenate copies of the password together to create a string  $P$  of length  $v \cdot \lceil p/v \rceil$  bits (the final  
1680 copy of the password may be truncated to create  $P$ ). Note that if the password is the empty string,  
1681 then so is  $P$ .
- 1682 4. Set  $I=S||P$  to be the concatenation of  $S$  and  $P$ .
- 1683 5. Set  $j=\lceil n/u \rceil$ .
- 1684 6. For  $i=1, 2, \dots, j$ , do the following:
  - 1685 a. Set  $A_i=H_c(D||I)$ , the  $i$ th hash of  $D||I$ . That is, compute the hash of  $D||I$ ; compute the hash  
1686 of that hash; etc.; continue in this fashion until a total of  $c$  hashes have been computed,  
1687 each on the result of the previous hash.
  - 1688 b. Concatenate copies of  $A_i$  to create a string  $B$  of length  $v$  bits (the final copy of  $A_i$  may be  
1689 truncated to create  $B$ ).
  - 1690 c. Treating  $I$  as a concatenation  $I_0, I_1, \dots, I_{k-1}$  of  $v$ -bit blocks, where  $k=\lceil s/v \rceil + \lceil p/v \rceil$ , modify  $I$   
1691 by setting  $I_j=(I_j+B+1) \bmod 2^v$  for each  $j$ . To perform this addition, treat each  $v$ -bit block as  
1692 a binary number represented most-significant bit first.
- 1693 7. Concatenate  $A_1, A_2, \dots, A_j$  together to form a pseudo-random bit string,  $A$ .
- 1694 8. Use the first  $n$  bits of  $A$  as the output of this entire process

1695 When the password-based encryption mechanisms presented in this section are used to generate a key  
1696 and IV (if needed) from a password, salt, and an iteration count, the above algorithm is used. To  
1697 generate a key, the identifier byte  $ID$  is set to the value 1; to generate an IV, the identifier byte  $ID$  is set to  
1698 the value 2.

1699 When the password-based authentication mechanism presented in this section is used to generate a key  
1700 from a password, salt and an iteration count, the above algorithm is used. The identifier  $ID$  is set to the  
1701 value 3.

### 1702 2.14.1 SHA-1-PBE for 128-bit RC4

1703 SHA-1-PBE for 128-bit RC4, denoted **CKM\_PBE\_SHA1\_RC4\_128**, is a mechanism used for generating  
1704 a 128-bit RC4 secret key from a password and a salt value by using the SHA-1 digest algorithm and an  
1705 iteration count. The method used to generate the key is described above.

1706 It has a parameter, a **CK\_PBE\_PARAMS** structure. The parameter specifies the input information for the  
1707 key generation process. The parameter also has a field to hold the location of an application-supplied  
1708 buffer which will receive an IV; for this mechanism, the contents of this field are ignored, since RC4 does  
1709 not require an IV.

1710 The key produced by this mechanism will typically be used for performing password-based encryption.

### 1711 **2.14.2 SHA-1\_PBE for 40-bit RC4**

1712 SHA-1-PBE for 40-bit RC4, denoted **CKM\_PBE\_SHA1\_RC4\_40**, is a mechanism used for generating a  
1713 40-bit RC4 secret key from a password and a salt value by using the SHA-1 digest algorithm and an  
1714 iteration count. The method used to generate the key is described above.

1715 It has a parameter, a **CK\_PBE\_PARAMS** structure. The parameter specifies the input information for the  
1716 key generation process. The parameter also has a field to hold the location of an application-supplied  
1717 buffer which will receive an IV; for this mechanism, the contents of this field are ignored, since RC4 does  
1718 not require an IV.

1719 The key produced by this mechanism will typically be used for performing password-based encryption.

### 1720 **2.14.3 SHA-1\_PBE for 128-bit RC2-CBC**

1721 SHA-1-PBE for 128-bit RC2-CBC, denoted **CKM\_PBE\_SHA1\_RC2\_128\_CBC**, is a mechanism used for  
1722 generating a 128-bit RC2 secret key from a password and a salt value by using the SHA-1 digest  
1723 algorithm and an iteration count. The method used to generate the key and IV is described above.

1724 It has a parameter, a **CK\_PBE\_PARAMS** structure. The parameter specifies the input information for the  
1725 key generation process and the location of an application-supplied buffer which will receive the 8-byte IV  
1726 generated by the mechanism.

1727 When the key and IV generated by this mechanism are used to encrypt or decrypt, the effective number  
1728 of bits in the RC2 search space should be set to 128. This ensures compatibility with the ASN.1 Object  
1729 Identifier `pbeWithSHA1And128BitRC2-CBC`.

1730 The key and IV produced by this mechanism will typically be used for performing password-based  
1731 encryption.

### 1732 **2.14.4 SHA-1\_PBE for 40-bit RC2-CBC**

1733 SHA-1-PBE for 40-bit RC2-CBC, denoted **CKM\_PBE\_SHA1\_RC2\_40\_CBC**, is a mechanism used for  
1734 generating a 40-bit RC2 secret key from a password and a salt value by using the SHA-1 digest algorithm  
1735 and an iteration count. The method used to generate the key and IV is described above.

1736 It has a parameter, a **CK\_PBE\_PARAMS** structure. The parameter specifies the input information for the  
1737 key generation process and the location of an application-supplied buffer which will receive the 8-byte IV  
1738 generated by the mechanism.

1739 When the key and IV generated by this mechanism are used to encrypt or decrypt, the effective number  
1740 of bits in the RC2 search space should be set to 40. This ensures compatibility with the ASN.1 Object  
1741 Identifier `pbeWithSHA1And40BitRC2-CBC`.

1742 The key and IV produced by this mechanism will typically be used for performing password-based  
1743 encryption

## 1744 **2.15 RIPE-MD**

### 1745 **2.15.1 Definitions**

1746 Mechanisms:

1747 **CKM\_RIPEMD128**

1748 **CKM\_RIPEMD128\_HMAC**

1749 **CKM\_RIPEMD128\_HMAC\_GENERAL**

1750 **CKM\_RIPEMD160**

1751 **CKM\_RIPEMD160\_HMAC**

1752 **CKM\_RIPEMD160\_HMAC\_GENERAL**

1753 **2.15.2 RIPE-MD 128 Digest**

1754 The RIPE-MD 128 mechanism, denoted **CKM\_RIPEMD128**, is a mechanism for message digesting,  
1755 following the RIPE-MD 128 message-digest algorithm.

1756 It does not have a parameter.

1757 Constraints on the length of data are summarized in the following table:

1758 *Table 55, RIPE-MD 128: Data Length*

Function	Data length	Digest length
C_Digest	Any	16

1759

1760 **2.15.3 General-length RIPE-MD 128-HMAC**

1761 The general-length RIPE-MD 128-HMAC mechanism, denoted **CKM\_RIPEMD128\_HMAC\_GENERAL**, is  
1762 a mechanism for signatures and verification. It uses the HMAC construction, based on the RIPE-MD 128  
1763 hash function. The keys it uses are generic secret keys.

1764 It has a parameter, a **CK\_MAC\_GENERAL\_PARAMS**, which holds the length in bytes of the desired  
1765 output. This length should be in the range 0-16 (the output size of RIPE-MD 128 is 16 bytes). Signatures  
1766 (MACs) produced by this mechanism will be taken from the start of the full 16-byte HMAC output.

1767 *Table 56, General-length RIPE-MD 128-HMAC*

Function	Key type	Data length	Signature length
C_Sign	Generic secret	Any	0-16, depending on parameters
C_Verify	Generic secret	Any	0-16, depending on parameters

1768 **2.15.4 RIPE-MD 128-HMAC**

1769 The RIPE-MD 128-HMAC mechanism, denoted **CKM\_RIPEMD128\_HMAC**, is a special case of the  
1770 general-length RIPE-MD 128-HMAC mechanism in Section 2.15.3.

1771 It has no parameter, and always produces an output of length 16.

1772 **2.15.5 RIPE-MD 160**

1773 The RIPE-MD 160 mechanism, denoted **CKM\_RIPEMD160**, is a mechanism for message digesting,  
1774 following the RIPE-MD 160 message-digest defined in ISO-10118.

1775 It does not have a parameter.

1776 Constraints on the length of data are summarized in the following table:

1777 *Table 57, RIPE-MD 160: Data Length*

Function	Data length	Digest length
C_Digest	Any	20

1778 **2.15.6 General-length RIPE-MD 160-HMAC**

1779 The general-length RIPE-MD 160-HMAC mechanism, denoted **CKM\_RIPEMD160\_HMAC\_GENERAL**, is  
1780 a mechanism for signatures and verification. It uses the HMAC construction, based on the RIPE-MD 160  
1781 hash function. The keys it uses are generic secret keys.

1782 It has a parameter, a **CK\_MAC\_GENERAL\_PARAMS**, which holds the length in bytes of the desired  
 1783 output. This length should be in the range 0-20 (the output size of RIPE-MD 160 is 20 bytes). Signatures  
 1784 (MACs) produced by this mechanism will be taken from the start of the full 20-byte HMAC output.

1785 *Table 58, General-length RIPE-MD 160-HMAC: Data and Length*

Function	Key type	Data length	Signature length
C_Sign	Generic secret	Any	0-20, depending on parameters
C_Verify	Generic secret	Any	0-20, depending on parameters

## 1786 2.15.7 RIPE-MD 160-HMAC

1787 The RIPE-MD 160-HMAC mechanism, denoted **CKM\_RIPEMD160\_HMAC**, is a special case of the  
 1788 general-length RIPE-MD 160HMAC mechanism in Section 2.15.6.

1789 It has no parameter, and always produces an output of length 20.

## 1790 2.16 SET

### 1791 2.16.1 Definitions

1792 Mechanisms:

1793 **CKM\_KEY\_WRAP\_SET\_OAEP**

### 1794 2.16.2 SET mechanism parameters

#### 1795 2.16.2.1 CK\_KEY\_WRAP\_SET\_OAEP\_PARAMS; 1796 CK\_KEY\_WRAP\_SET\_OAEP\_PARAMS\_PTR

1797 **CK\_KEY\_WRAP\_SET\_OAEP\_PARAMS** is a structure that provides the parameters to the  
 1798 **CKM\_KEY\_WRAP\_SET\_OAEP** mechanism. It is defined as follows:

```
1799 typedef struct CK_KEY_WRAP_SET_OAEP_PARAMS {
1800     CK_BYTE bBC;
1801     CK_BYTE_PTR pX;
1802     CK_ULONG ulXLen;
1803 } CK_KEY_WRAP_SET_OAEP_PARAMS;
```

1804 The fields of the structure have the following meanings:

1805 *bBC* block contents byte

1806 *pX* concatenation of hash of plaintext data (if present) and  
 1807 extra data (if present)

1808 *ulXLen* length in bytes of concatenation of hash of plaintext data  
 1809 (if present) and extra data (if present). 0 if neither is  
 1810 present.

1811 **CK\_KEY\_WRAP\_SET\_OAEP\_PARAMS\_PTR** is a pointer to a  
 1812 **CK\_KEY\_WRAP\_SET\_OAEP\_PARAMS**.

### 1813 2.16.3 OAEP key wrapping for SET

1814 The OAEP key wrapping for SET mechanism, denoted **CKM\_KEY\_WRAP\_SET\_OAEP**, is a mechanism  
 1815 for wrapping and unwrapping a DES key with an RSA key. The hash of some plaintext data and/or some

1816 extra data may optionally be wrapped together with the DES key. This mechanism is defined in the SET  
1817 protocol specifications.

1818 It takes a parameter, a **CK\_KEY\_WRAP\_SET\_OAEP\_PARAMS** structure. This structure holds the  
1819 “Block Contents” byte of the data and the concatenation of the hash of plaintext data (if present) and the  
1820 extra data to be wrapped (if present). If neither the hash nor the extra data is present, this is indicated by  
1821 the *ulXLen* field having the value 0.

1822 When this mechanism is used to unwrap a key, the concatenation of the hash of plaintext data (if present)  
1823 and the extra data (if present) is returned following the convention described in Section \*\*\*MISSING  
1824 REFERENCE\*\*\* on producing output. Note that if the inputs to **C\_UnwrapKey** are such that the extra  
1825 data is not returned (e.g. the buffer supplied in the **CK\_KEY\_WRAP\_SET\_OAEP\_PARAMS** structure is  
1826 NULL\_PTR), then the unwrapped key object will not be created, either.

1827 Be aware that when this mechanism is used to unwrap a key, the *bBC* and *pX* fields of the parameter  
1828 supplied to the mechanism may be modified.

1829 If an application uses **C\_UnwrapKey** with **CKM\_KEY\_WRAP\_SET\_OAEP**, it may be preferable for it  
1830 simply to allocate a 128-byte buffer for the concatenation of the hash of plaintext data and the extra data  
1831 (this concatenation is never larger than 128 bytes), rather than calling **C\_UnwrapKey** twice. Each call of  
1832 **C\_UnwrapKey** with **CKM\_KEY\_WRAP\_SET\_OAEP** requires an RSA decryption operation to be  
1833 performed, and this computational overhead can be avoided by this means.

## 1834 2.17 LYNKS

### 1835 2.17.1 Definitions

1836 Mechanisms:

1837 **CKM\_KEY\_WRAP\_LYNKS**

### 1838 2.17.2 LYNKS key wrapping

1839 The LYNKS key wrapping mechanism, denoted **CKM\_KEY\_WRAP\_LYNKS**, is a mechanism for  
1840 wrapping and unwrapping secret keys with DES keys. It can wrap any 8-byte secret key, and it produces  
1841 a 10-byte wrapped key, containing a cryptographic checksum.

1842 It does not have a parameter.

1843 To wrap an 8-byte secret key *K* with a DES key *W*, this mechanism performs the following steps:

- 1844 1. Initialize two 16-bit integers,  $sum_1$  and  $sum_2$ , to 0
- 1845 2. Loop through the bytes of *K* from first to last.
- 1846 3. Set  $sum_1 = sum_1 +$  the key byte (treat the key byte as a number in the range 0-255).
- 1847 4. Set  $sum_2 = sum_2 + sum_1$ .
- 1848 5. Encrypt *K* with *W* in ECB mode, obtaining an encrypted key, *E*.
- 1849 6. Concatenate the last 6 bytes of *E* with  $sum_2$ , representing  $sum_2$  most-significant bit first. The  
1850 result is an 8-byte block, *T*
- 1851 7. Encrypt *T* with *W* in ECB mode, obtaining an encrypted checksum, *C*.
- 1852 8. Concatenate *E* with the last 2 bytes of *C* to obtain the wrapped key.

1853 When unwrapping a key with this mechanism, if the cryptographic checksum does not check out properly,  
1854 an error is returned. In addition, if a DES key or CDMF key is unwrapped with this mechanism, the parity  
1855 bits on the wrapped key must be set appropriately. If they are not set properly, an error is returned.

1856

---

1857 **3 PKCS #11 Implementation Conformance**

1858 An implementation is a conforming implementation if it meets the conditions specified in one or more  
1859 server profiles specified in **[PKCS #11-Prof]**.

1860 A PKCS #11 implementation SHALL be a conforming PKCS #11 implementation.

1861 If a PKCS #11 implementation claims support for a particular profile, then the implementation SHALL  
1862 conform to all normative statements within the clauses specified for that profile and for any subclauses to  
1863 each of those clauses .

1864

---

## 1865 Appendix A. Acknowledgments

1866 The following individuals have participated in the creation of this specification and are gratefully  
1867 acknowledged:

1868

1869 **Participants:**

1870 Gil Abel, Athena Smartcard Solutions, Inc.

1871 Warren Armstrong, QuintessenceLabs

1872 Peter Bartok, Venafi, Inc.

1873 Anthony Berglas, Cryptsoft

1874 Kelley Burgin, National Security Agency

1875 Robert Burns, Thales e-Security

1876 Wan-Teh Chang, Google Inc.

1877 Hai-May Chao, Oracle

1878 Janice Cheng, Vormetric, Inc.

1879 Sangrae Cho, Electronics and Telecommunications Research Institute (ETRI)

1880 Doron Cohen, SafeNet, Inc.

1881 Fadi Cotran, Futurex

1882 Tony Cox, Cryptsoft

1883 Christopher Duane, EMC

1884 Chris Dunn, SafeNet, Inc.

1885 Valerie Fenwick, Oracle

1886 Terry Fletcher, SafeNet, Inc.

1887 Susan Gleeson, Oracle

1888 Sven Gossel, Charismathics

1889 Robert Griffin, EMC

1890 Paul Grojean, Individual

1891 Peter Gutmann, Individual

1892 Dennis E. Hamilton, Individual

1893 Thomas Hardjono, M.I.T.

1894 Tim Hudson, Cryptsoft

1895 Gershon Janssen, Individual

1896 Seunghun Jin, Electronics and Telecommunications Research Institute (ETRI)

1897 Andrey Jivsov, Symantec Corp.

1898 Greg Kazmierczak, Wave Systems Corp.

1899 Mark Knight, Thales e-Security

1900 Darren Krahn, Google Inc.

1901 Alex Krasnov, Infineon Technologies AG

1902 Dina Kurktchi-Nimeh, Oracle

1903 Mark Lambiase, SecureAuth Corporation

1904 Lawrence Lee, GoTrust Technology Inc.



1905 John Leiseboer, QuintessenceLabs  
1906 Hal Lockhart, Oracle  
1907 Robert Lockhart, Thales e-Security  
1908 Dale Moberg, Axway Software  
1909 Darren Moffat, Oracle  
1910 Valery Osheter, SafeNet, Inc.  
1911 Sean Parkinson, EMC  
1912 Rob Philpott, EMC  
1913 Mark Powers, Oracle  
1914 Ajai Puri, SafeNet, Inc.  
1915 Robert Relyea, Red Hat  
1916 Saikat Saha, Oracle  
1917 Subhash Sankuratripati, NetApp  
1918 Johann Schoetz, Infineon Technologies AG  
1919 Rayees Shamsuddin, Wave Systems Corp.  
1920 Radhika Siravara, Oracle  
1921 Brian Smith, Mozilla Corporation  
1922 David Smith, Venafi, Inc.  
1923 Ryan Smith, Futurex  
1924 Jerry Smith, US Department of Defense (DoD)  
1925 Oscar So, Oracle  
1926 Michael Stevens, QuintessenceLabs  
1927 Michael StJohns, Individual  
1928 Sander Temme, Thales e-Security  
1929 Kiran Thota, VMware, Inc.  
1930 Walter-John Turnes, Gemini Security Solutions, Inc.  
1931 Stef Walter, Red Hat  
1932 Jeff Webb, Dell  
1933 Magda Zdunkiewicz, Cryptsoft  
1934 Chris Zimman, Bloomberg Finance L.P.

1935

## Appendix B. Manifest constants

1936 The following constants have been defined for PKCS #11 V2.40. Also, refer to **[PKCS #11-Base]** and  
1937 **[PKCS #11-Curr]** for additional definitions.

```
1938 /*  
1939 * Copyright OASIS Open 2013. All rights reserved.  
1940 * OASIS trademark, IPR and other policies apply.  
1941 * http://www.oasis-open.org/policies-guidelines/ipr  
1942 */  
1943  
1944 #define CKK_KEA 0x00000005  
1945 #define CKK_RC2 0x00000011  
1946 #define CKK_RC4 0x00000012  
1947 #define CKK_DES 0x00000013  
1948 #define CKK_CAST 0x00000016  
1949 #define CKK_CAST3 0x00000017  
1950 #define CKK_CAST5 0x00000018  
1951 #define CKK_CAST128 0x00000018  
1952 #define CKK_RC5 0x00000019  
1953 #define CKK_IDEA 0x0000001A  
1954 #define CKK_SKIPJACK 0x0000001B  
1955 #define CKK_BATON 0x0000001C  
1956 #define CKK_JUNIPER 0x0000001D  
1957 #define CKM_MD2_RSA_PKCS 0x00000004  
1958 #define CKM_MD5_RSA_PKCS 0x00000005  
1959 #define CKM_RIPEMD128_RSA_PKCS 0x00000007  
1960 #define CKM_RIPEMD160_RSA_PKCS 0x00000008  
1961 #define CKM_RC2_KEY_GEN 0x00000100  
1962 #define CKM_RC2_ECB 0x00000101  
1963 #define CKM_RC2_CBC 0x00000102  
1964 #define CKM_RC2_MAC 0x00000103  
1965 #define CKM_RC2_MAC_GENERAL 0x00000104  
1966 #define CKM_RC2_CBC_PAD 0x00000105  
1967 #define CKM_RC4_KEY_GEN 0x00000110  
1968 #define CKM_RC4 0x00000111  
1969 #define CKM_DES_KEY_GEN 0x00000120  
1970 #define CKM_DES_ECB 0x00000121  
1971 #define CKM_DES_CBC 0x00000122  
1972 #define CKM_DES_MAC 0x00000123  
1973 #define CKM_DES_MAC_GENERAL 0x00000124  
1974 #define CKM_DES_CBC_PAD 0x00000125  
1975 #define CKM_MD2 0x00000200  
1976 #define CKM_MD2_HMAC 0x00000201  
1977 #define CKM_MD2_HMAC_GENERAL 0x00000202  
1978 #define CKM_MD5 0x00000210  
1979 #define CKM_MD5_HMAC 0x00000211  
1980 #define CKM_MD5_HMAC_GENERAL 0x00000212  
1981 #define CKM_RIPEMD128 0x00000230  
1982 #define CKM_RIPEMD128_HMAC 0x00000231  
1983 #define CKM_RIPEMD128_HMAC_GENERAL 0x00000232  
1984 #define CKM_RIPEMD160 0x00000240  
1985 #define CKM_RIPEMD160_HMAC 0x00000241  
1986 #define CKM_RIPEMD160_HMAC_GENERAL 0x00000242  
1987 #define CKM_CAST_KEY_GEN 0x00000300  
1988 #define CKM_CAST_ECB 0x00000301  
1989 #define CKM_CAST_CBC 0x00000302  
1990 #define CKM_CAST_MAC 0x00000303  
1991 #define CKM_CAST_MAC_GENERAL 0x00000304  
1992 #define CKM_CAST_CBC_PAD 0x00000305  
1993 #define CKM_CAST3_KEY_GEN 0x00000310
```

```

1994 #define CKM_CAST3_ECB 0x00000311
1995 #define CKM_CAST3_CBC 0x00000312
1996 #define CKM_CAST3_MAC 0x00000313
1997 #define CKM_CAST3_MAC_GENERAL 0x00000314
1998 #define CKM_CAST3_CBC_PAD 0x00000315
1999 #define CKM_CAST5_KEY_GEN 0x00000320
2000 #define CKM_CAST128_KEY_GEN 0x00000320
2001 #define CKM_CAST5_ECB 0x00000321
2002 #define CKM_CAST128_ECB 0x00000321
2003 #define CKM_CAST5_CBC 0x00000322
2004 #define CKM_CAST128_CBC 0x00000322
2005 #define CKM_CAST5_MAC 0x00000323
2006 #define CKM_CAST128_MAC 0x00000323
2007 #define CKM_CAST5_MAC_GENERAL 0x00000324
2008 #define CKM_CAST128_MAC_GENERAL 0x00000324
2009 #define CKM_CAST5_CBC_PAD 0x00000325
2010 #define CKM_CAST128_CBC_PAD 0x00000325
2011 #define CKM_RC5_KEY_GEN 0x00000330
2012 #define CKM_RC5_ECB 0x00000331
2013 #define CKM_RC5_CBC 0x00000332
2014 #define CKM_RC5_MAC 0x00000333
2015 #define CKM_RC5_MAC_GENERAL 0x00000334
2016 #define CKM_RC5_CBC_PAD 0x00000335
2017 #define CKM_IDEA_KEY_GEN 0x00000340
2018 #define CKM_IDEA_ECB 0x00000341
2019 #define CKM_IDEA_CBC 0x00000342
2020 #define CKM_IDEA_MAC 0x00000343
2021 #define CKM_IDEA_MAC_GENERAL 0x00000344
2022 #define CKM_IDEA_CBC_PAD 0x00000345
2023 #define CKM_MD5_KEY_DERIVATION 0x00000390
2024 #define CKM_MD2_KEY_DERIVATION 0x00000391
2025 #define CKM_PBE_MD2_DES_CBC 0x000003A0
2026 #define CKM_PBE_MD5_DES_CBC 0x000003A1
2027 #define CKM_PBE_MD5_CAST_CBC 0x000003A2
2028 #define CKM_PBE_MD5_CAST3_CBC 0x000003A3
2029 #define CKM_PBE_MD5_CAST5_CBC 0x000003A4
2030 #define CKM_PBE_MD5_CAST128_CBC 0x000003A4
2031 #define CKM_PBE_SHA1_CAST5_CBC 0x000003A5
2032 #define CKM_PBE_SHA1_CAST128_CBC 0x000003A5
2033 #define CKM_PBE_SHA1_RC4_128 0x000003A6
2034 #define CKM_PBE_SHA1_RC4_40 0x000003A7
2035 #define CKM_PBE_SHA1_RC2_128_CBC 0x000003AA
2036 #define CKM_PBE_SHA1_RC2_40_CBC 0x000003AB
2037 #define CKM_KEY_WRAP_LYNKS 0x00000400
2038 #define CKM_KEY_WRAP_SET_OAEP 0x00000401
2039 #define CKM_SKIPJACK_KEY_GEN 0x00001000
2040 #define CKM_SKIPJACK_ECB64 0x00001001
2041 #define CKM_SKIPJACK_CBC64 0x00001002
2042 #define CKM_SKIPJACK_OFB64 0x00001003
2043 #define CKM_SKIPJACK_CFB64 0x00001004
2044 #define CKM_SKIPJACK_CFB32 0x00001005
2045 #define CKM_SKIPJACK_CFB16 0x00001006
2046 #define CKM_SKIPJACK_CFB8 0x00001007
2047 #define CKM_SKIPJACK_WRAP 0x00001008
2048 #define CKM_SKIPJACK_PRIVATE_WRAP 0x00001009
2049 #define CKM_SKIPJACK_RELAYX 0x0000100a
2050 #define CKM_KEA_KEY_PAIR_GEN 0x00001010
2051 #define CKM_KEA_KEY_DERIVE 0x00001011
2052 #define CKM_FORTEZZA_TIMESTAMP 0x00001020
2053 #define CKM_BATON_KEY_GEN 0x00001030
2054 #define CKM_BATON_ECB128 0x00001031
2055 #define CKM_BATON_ECB96 0x00001032
2056 #define CKM_BATON_CBC128 0x00001033
2057 #define CKM_BATON_COUNTER 0x00001034

```

```
2058 #define CKM_BATON_SHUFFLE 0x00001035
2059 #define CKM_BATON_WRAP 0x00001036
2060 #define CKM_JUNIPER_KEY_GEN 0x00001060
2061 #define CKM_JUNIPER_ECB128 0x00001061
2062 #define CKM_JUNIPER_CBC128 0x00001062
2063 #define CKM_JUNIPER_COUNTER 0x00001063
2064 #define CKM_JUNIPER_SHUFFLE 0x00001064
2065 #define CKM_JUNIPER_WRAP 0x00001065
2066 #define CKM_FASTHASH 0x00001070
```

2067

2068

---

## Appendix C. Revision History

2069

<b>Revision</b>	<b>Date</b>	<b>Editor</b>	<b>Changes Made</b>
wd01	May 16, 2013	Susan Gleeson	Initial Template import
wd02	July 7, 2013	Susan Gleeson	Fix references, add participants list, minor cleanup
wd03	October 27, 2013	Robert Griffin	Final participant list and other editorial changes for Committee Specification Draft

2070

2071