

SafeNet Luna PCIe HSM Client 10.1

SDK REFERENCE GUIDE



Document Information

Product Version	10.1
Document Part Number	007-000555-001
Release Date	23 January 2020

Revision History

Revision	Date	Reason
Rev. A	23 January 2020	Initial release

Trademarks, Copyrights, and Third-Party Software

Copyright 2001-2020 Thales. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales's information.

This document can be used for informational, non-commercial, internal, and personal use only provided that:

- > The copyright notice, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- > This document shall not be posted on any publicly accessible network computer or broadcast in any media, and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential

damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service, or loss of privacy.

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of Thales Group.

Regulatory Compliance

This product complies with the following regulatory regulations. To ensure compliancy, ensure that you install the products as specified in the installation instructions and use only Thales-supplied or approved accessories.

USA, FCC

This equipment has been tested and found to comply with the limits for a “Class B” digital device, pursuant to part 15 of the FCC rules.

Canada

This class B digital apparatus meets all requirements of the Canadian interference-causing equipment regulations.

Europe

This product is in conformity with the protection requirements of EC Council Directive 2014/30/EU. This product satisfies the CLASS B limits of EN55032.

CONTENTS

Preface: About the SDK Reference Guide	13
Customer Release Notes	13
Audience	13
Document Conventions	14
Support Contacts	16
Chapter 1: SafeNet SDK Overview	17
Supported Cryptographic Algorithms	17
Application Programming Interface (API) Overview	17
Sample Application	18
A Note About RSA Key Attributes 'p' and 'q'	19
What Does 'Supported' Mean?	19
Why Is an Integration Not Listed Here Or On the Website?	20
Frequently Asked Questions	20
Chapter 2: PKCS#11 Support	23
PKCS#11 Compliance	23
Supported PKCS#11 Services	23
Additional Functions	27
Using the PKCS#11 Sample	27
The SfmtLibPath Environment Variable	27
What p11Sample Does	27
Chapter 3: Extensions to PKCS#11	29
SafeNet Luna Extensions to PKCS#11	29
HSM Configuration Settings	40
Secure PIN Port Authentication	40
High Availability Indirect Login Functions	41
Initialization functions	41
Recovery Functions	41
Login Key Attributes	43
Control of HA Functionality	44
MofN Secret Sharing (quorum or multi-person access control)	44
Key Export Features	44
RSA Key Component Wrapping	44
Derivation of Symmetric Keys with 3DES_ECB	47
PKCS#11 Extension HA Status Call	47
Function Definition	47
Counter Mode KDF Mechanisms	48
BIP32 Mechanism Support and Implementation	48
Curve Support	48

Key Type and Form	49
Extended Keys and Hardened Keys	49
Key Derivation	49
Error Codes	50
Key Attributes	50
Public Key Import/Export	51
Private Key Import/Export	52
Key Backup and Cloning	53
Non-FIPS Algorithm	53
Host Tools	53
Code Samples	53
Derive Template	56
Examples	57

Chapter 4: Supported Mechanisms

CKM_AES_CBC	59
CKM_AES_CBC_ENCRYPT_DATA	60
CKM_AES_CBC_PAD	61
CKM_AES_CBC_PAD_IPSEC	62
CKM_AES_CFB8	63
CKM_AES_CFB128	64
CKM_AES_CMAC	65
CKM_AES_CMAC_GENERAL	66
CKM_AES_CTR	67
CKM_AES_ECB	68
CKM_AES_ECB_ENCRYPT_DATA	69
CKM_AES_GCM	70
CKM_AES_GMAC	72
CKM_AES_KEY_GEN	74
CKM_AES_KW	75
CKM_AES_KWP	76
CKM_AES_MAC	77
CKM_AES_MAC_GENERAL	78
CKM_AES_OFB	79
CKM_AES_XTS	80
CKM_ARIA_CBC	81
CKM_ARIA_CBC_ENCRYPT_DATA	82
CKM_ARIA_CBC_PAD	83
CKM_ARIA_CFB8	84
CKM_ARIA_CFB128	85
CKM_ARIA_CMAC	86
CKM_ARIA_CMAC_GENERAL	87
CKM_ARIA_CTR	88
CKM_ARIA_ECB	89
CKM_ARIA_ECB_ENCRYPT_DATA	90
CKM_ARIA_KEY_GEN	91
CKM_ARIA_L_CBC	92

CKM_ARIA_L_CBC_PAD	93
CKM_ARIA_L_ECB	94
CKM_ARIA_L_MAC	95
CKM_ARIA_L_MAC_GENERAL	96
CKM_ARIA_MAC	97
CKM_ARIA_MAC_GENERAL	98
CKM_ARIA_OFB	99
CKM_BIP32_CHILD_DERIVE	100
CKM_BIP32_MASTER_DERIVE	101
CKM_CAST3_CBC	102
CKM_CAST3_CBC_PAD	103
CKM_CAST3_ECB	104
CKM_CAST3_KEY_GEN	105
CKM_CAST3_MAC	106
CKM_CAST3_MAC_GENERAL	107
CKM_CAST5_CBC	108
CKM_CAST5_CBC_PAD	109
CKM_CAST5_ECB	110
CKM_CAST5_KEY_GEN	111
CKM_CAST5_MAC	112
CKM_CAST5_MAC_GENERAL	113
CKM_DES_CBC	114
CKM_DES_CBC_ENCRYPT_DATA	115
CKM_DES_CBC_PAD	116
CKM_DES_CFB8	117
CKM_DES_CFB64	118
CKM_DES_ECB	119
CKM_DES_ECB_ENCRYPT_DATA	120
CKM_DES_KEY_GEN	121
CKM_DES_MAC	122
CKM_DES_MAC_GENERAL	123
CKM_DES_OFB64	124
CKM_DES2_DUKPT_DATA	125
CKM_DES2_DUKPT_DATA_RESP	127
CKM_DES2_DUKPT_MAC	129
CKM_DES2_DUKPT_MAC_RESP	131
CKM_DES2_DUKPT_PIN	133
CKM_DES2_KEY_GEN	135
CKM_DES3_CBC	136
CKM_DES3_CBC_ENCRYPT_DATA	137
CKM_DES3_CBC_PAD	138
CKM_DES3_CBC_PAD_IPSEC	139
CKM_DES3_CMAC	140
CKM_DES3_CMAC_GENERAL	141
CKM_DES3_CTR	142
CKM_DES3_ECB	143
CKM_DES3_ECB_ENCRYPT_DATA	144

CKM_DES3_KEY_GEN	145
CKM_DES3_MAC	146
CKM_DES3_MAC_GENERAL	147
CKM_DES3_X919_MAC	148
CKM_DH_PKCS_DERIVE	150
CKM_DH_PKCS_KEY_PAIR_GEN	151
CKM_DH_PKCS_PARAMETER_GEN	152
CKM_DSA	153
CKM_DSA_KEY_PAIR_GEN	154
CKM_DSA_PARAMETER_GEN	155
CKM_DSA_SHA1	156
CKM_DSA_SHA224	157
CKM_DSA_SHA256	158
CKM_EC_EDWARDS_KEY_PAIR_GEN	159
CKM_EC_KEY_PAIR_GEN	160
CKM_EC_KEY_PAIR_GEN_W_EXTRA_BITS	161
CKM_EC_MONTGOMERY_KEY_PAIR_GEN	162
CKM_ECDH1_COFACTOR_DERIVE	163
CKM_ECDH1_DERIVE	164
CKM_ECDSA	165
CKM_ECDSA_GBCS_SHA256	166
CKM_ECDSA_SHA1	167
CKM_ECDSA_SHA224	168
CKM_ECDSA_SHA256	169
CKM_ECDSA_SHA384	170
CKM_ECDSA_SHA512	171
CKM_ECIES	172
CKM_EDDSA	173
CKM_EDDSA_NACL	175
CKM_GENERIC_SECRET_KEY_GEN	176
CKM_HAS160	177
CKM_KCDSA_HAS160	178
CKM_KCDSA_HAS160_NO_PAD	179
CKM_KCDSA_KEY_PAIR_GEN	180
CKM_KCDSA_PARAMETER_GEN	181
CKM_KCDSA_SHA1	182
CKM_KCDSA_SHA1_NO_PAD	183
CKM_KCDSA_SHA224	184
CKM_KCDSA_SHA224_NO_PAD	185
CKM_KCDSA_SHA256	186
CKM_KCDSA_SHA256_NO_PAD	187
CKM_KCDSA_SHA384	188
CKM_KCDSA_SHA384_NO_PAD	189
CKM_KCDSA_SHA512	190
CKM_KCDSA_SHA512_NO_PAD	191
CKM_KEY_WRAP_SET_OAEP	192
CKM_MD2	193

CKM_MD2_KEY_DERIVATION	194
CKM_MD5_HMAC	195
CKM_MD5_HMAC_GENERAL	196
CKM_MD5_KEY_DERIVATION	197
CKM_NIST_PRF_KDF	198
CKM_PBE_MD2_DES_CBC	200
CKM_PBE_SHA1_CAST5_CBC	201
CKM_PBE_SHA1_DES2_EDE_CBC	202
CKM_PBE_SHA1_DES2_EDE_CBC_OLD	203
CKM_PBE_SHA1_DES3_EDE_CBC	204
CKM_PBE_SHA1_DES3_EDE_CBC_OLD	205
CKM_PBE_SHA1_RC2_40_CBC	206
CKM_PBE_SHA1_RC2_128_CBC	207
CKM_PBE_SHA1_RC4_40	208
CKM_PBE_SHA1_RC4_128	209
CKM_PKCS5_PBKD2	210
CKM_PRF_KDF	211
CKM_RC2_CBC	213
CKM_RC2_CBC_PAD	214
CKM_RC2_ECB	215
CKM_RC2_KEY_GEN	216
CKM_RC2_MAC	217
CKM_RC2_MAC_GENERAL	218
CKM_RC4	219
CKM_RC4_KEY_GEN	220
CKM_RC5_CBC	221
CKM_RC5_CBC_PAD	222
CKM_RC5_ECB	223
CKM_RC5_KEY_GEN	224
CKM_RC5_MAC	225
CKM_RC5_MAC_GENERAL	226
CKM_RSA_FIPS_186_3_AUX_PRIME_KEY_PAIR_GEN	227
CKM_RSA_FIPS_186_3_PRIME_KEY_PAIR_GEN	228
CKM_RSA_PKCS	229
CKM_RSA_PKCS_KEY_PAIR_GEN	230
CKM_RSA_PKCS_OAEP	231
CKM_RSA_PKCS_PSS	232
CKM_RSA_X_509	233
CKM_RSA_X9_31	234
CKM_RSA_X9_31_KEY_PAIR_GEN	235
CKM_RSA_X9_31_NON_FIPS	236
CKM_SEED_CBC	237
CKM_SEED_CBC_PAD	238
CKM_SEED_CMAC	239
CKM_SEED_CMAC_GENERAL	240
CKM_SEED_CTR	241
CKM_SEED_ECB	242

CKM_SEED_KEY_GEN	243
CKM_SEED_MAC	244
CKM_SEED_MAC_GENERAL	245
CKM_SHA_1	246
CKM_SHA_1_HMAC	247
CKM_SHA_1_HMAC_GENERAL	248
CKM_SHA1_EDDSA	249
CKM_SHA1_EDDSA_NACL	250
CKM_SHA1_KEY_DERIVATION	251
CKM_SHA1_RSA_PKCS	252
CKM_SHA1_RSA_PKCS_PSS	253
CKM_SHA1_RSA_X9_31	254
CKM_SHA1_RSA_X9_31_NON_FIPS	255
CKM_SHA224	256
CKM_SHA224_EDDSA	257
CKM_SHA224_EDDSA_NACL	258
CKM_SHA224_HMAC	259
CKM_SHA224_HMAC_GENERAL	260
CKM_SHA224_KEY_DERIVATION	261
CKM_SHA224_RSA_PKCS	262
CKM_SHA224_RSA_PKCS_PSS	263
CKM_SHA224_RSA_X9_31	264
CKM_SHA224_RSA_X9_31_NON_FIPS	265
CKM_SHA256	266
CKM_SHA256_EDDSA	267
CKM_SHA256_EDDSA_NACL	268
CKM_SHA256_HMAC	269
CKM_SHA256_HMAC_GENERAL	270
CKM_SHA256_KEY_DERIVATION	271
CKM_SHA256_RSA_PKCS	272
CKM_SHA256_RSA_PKCS_PSS	273
CKM_SHA256_RSA_X9_31	274
CKM_SHA256_RSA_X9_31_NON_FIPS	275
CKM_SHA384	276
CKM_SHA384_EDDSA	277
CKM_SHA384_EDDSA_NACL	278
CKM_SHA384_HMAC	279
CKM_SHA384_HMAC_GENERAL	280
CKM_SHA384_KEY_DERIVATION	281
CKM_SHA384_RSA_PKCS	282
CKM_SHA384_RSA_PKCS_PSS	283
CKM_SHA384_RSA_X9_31	284
CKM_SHA384_RSA_X9_31_NON_FIPS	285
CKM_SHA512	286
CKM_SHA512_EDDSA	287
CKM_SHA512_EDDSA_NACL	288
CKM_SHA512_HMAC	289

CKM_SHA512_HMAC_GENERAL	290
CKM_SHA512_KEY_DERIVATION	291
CKM_SHA512_RSA_PKCS	292
CKM_SHA512_RSA_PKCS_PSS	293
CKM_SHA512_RSA_X9_31	294
CKM_SHA512_RSA_X9_31_NON_FIPS	295
CKM_SM3	296
CKM_SM3_HMAC	297
CKM_SM3_HMAC_GENERAL	298
CKM_SM3_KEY_DERIVATION	299
CKM_SSL3_KEY_AND_MAC_DERIVE	300
CKM_SSL3_MASTER_KEY_DERIVE	301
CKM_SSL3_MD5_MAC	302
CKM_SSL3_PRE_MASTER_KEY_GEN	303
CKM_SSL3_SHA1_MAC	304
CKM_X9_42_DH_DERIVE	305
CKM_X9_42_DH_HYBRID_DERIVE	306
CKM_X9_42_DH_KEY_PAIR_GEN	307
CKM_X9_42_DH_PARAMETER_GEN	308
CKM_XOR_BASE_AND_DATA_W_KDF	309
Chapter 5: Using the SafeNet SDK	310
Libraries and Applications	310
SafeNet SDK Applications General Information	310
Compiler Tools	311
Using CKlog	312
Application IDs	314
Shared Login State and Application IDs	314
Named Curves and User-Defined Parameters	318
Curve Validation Limitations	318
Storing Domain Parameters	318
Using Domain Parameters	319
User Friendly Encoder	319
Application Interfaces	319
Supported ECC Curves	325
Capability and Policy Configuration Control Using the SafeNet API	328
HSM Capabilities and Policies	328
HSM Partition Capabilities and Policies	329
Policy Refinement	329
Policy Types	329
Querying and Modifying HSM Configuration	330
Connection Timeout	332
Linux and Unix Connection Timeout	332
Windows Connection Timeout	333
Chapter 6: Design Considerations	334
PED-Authenticated HSMs	334

About CKDemo with Luna PED	335
Interchangeability	335
Startup	336
Cloning of Tokens	336
High Availability (HA) Implementations	336
Detecting the Failure of an HA Member	337
Key Attribute Defaults	338
Vendor-defined key attributes	340
Object Usage Count	340
Migrating Keys From Software to a SafeNet Luna PCIe HSM	343
Other Formats of Key Material	345
Sample Program	345
Audit Logging	367
Audit Log Records	367
Audit Log Message Format	368
Log External	369
Chapter 7: Java Interfaces	370
SafeNet JSP Overview and Installation	370
Installation	371
JSP Registration	372
Post-Installation Tasks	373
SafeNet JSP Configuration	375
SafeNet Java Security Provider	375
Keytool	378
Cleaning Up	378
PKCS#11/JCA Interaction	378
The JCPROV PKCS#11 Java Wrapper	379
JCPROV Overview	379
Installing JCPROV	380
JCPROV Sample Programs	380
JCPROV Sample Classes	381
JCPROV API Documentation	385
Java or JSP Errors	385
Re-Establishing a Connection Between Your Java Application and SafeNet Luna PCIe HSM	386
Recovering From the Loss of All HA Members	386
When to Use the reinitialize Method	387
Why the Method Must Be Used	387
What Happens on the HSM	387
Using Java Keytool with SafeNet Luna PCIe HSM	389
Limitations	389
Keytool Usage and Examples	390
Import CA certificate	390
Generate private key	391
Create the CSR	392
Import client certificate	392
How to build a certificate with chain	393

Additional minor notes	393
Chapter 8: Microsoft Interfaces	395
SafeNet CSP Registration Utilities	395
register	395
ms2Luna	397
keymap	398
SafeNet KSP for CNG Registration Utilities	399
kspcmd	399
KspConfig	401
ms2Luna	402
ksputil	403
Algorithms Supported	403
SafeNet CSP Calls and Functions	404
Programming for SafeNet Luna PCIe HSM with SafeNet CSP	405
Algorithms	406

PREFACE: About the SDK Reference Guide

This document describes how to use the SafeNet SDK to create applications that interact with SafeNet Luna PCIe HSMs. It contains the following chapters:

- > "SafeNet SDK Overview" on page 17
- > "PKCS#11 Support" on page 23
- > "Extensions to PKCS#11" on page 29
- > "Supported Mechanisms" on page 59
- > "Using the SafeNet SDK" on page 310
- > "Design Considerations" on page 334
- > "Java Interfaces" on page 370
- > "Microsoft Interfaces" on page 395

The preface includes the following information about this document:

- > "Customer Release Notes" below
- > "Audience" below
- > "Document Conventions" on the next page
- > "Support Contacts" on page 16

For information regarding the document status and revision history, see "Document Information" on page 2.

Customer Release Notes

The customer release notes (CRN) provide important information about this release that is not included in the customer documentation. Read the CRN to fully understand the capabilities, limitations, and known issues for this release. You can view or download the latest version of the CRN from the Technical Support Customer Portal at <https://supportportal.gemalto.com>.

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet Luna HSM users and security officers, key manager administrators, and network administrators.

All products manufactured and distributed by Thales Group are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

It is assumed that the users of this document are proficient with security concepts.

Document Conventions

This document uses standard conventions for describing the user interface and for alerting you to important information.

Notes

Notes are used to alert you to important or helpful information. They use the following format:

NOTE Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. They use the following format:

CAUTION! Exercise caution. Contains important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. They use the following format:

****WARNING**** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Command syntax and typeface conventions

Format	Convention
bold	<p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"> > Command-line commands and options (Type dir /p.) > Button names (Click Save As.) > Check box and radio button names (Select the Print Duplex check box.) > Dialog box titles (On the Protect Document dialog box, click Yes.) > Field names (User Name: Enter the name of the user.) > Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) > User input (In the Date box, type April 1.)
<i>italics</i>	<p>In type, the italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)</p>

Format	Convention
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Represent optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
{ a b c } {<a> <c>}	Represent required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.
[a b c] [<a> <c>]	Represent optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or [Thales Customer Support](#).

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at <https://supportportal.gemalto.com>, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone

The support portal also lists telephone numbers for voice contact. ([KB0013367](#))

Email Support

You can also contact technical support by email at technical.support@gemalto.com.

CHAPTER 1: SafeNet SDK Overview

This chapter provides an overview of the SafeNet Software Development Kit (SDK), a development platform you can use to integrate a SafeNet Luna PCIe HSM into your application or system. It contains the following topics:

- > ["Supported Cryptographic Algorithms" below](#)
- > ["Application Programming Interface \(API\) Overview" below](#)
- > ["What Does 'Supported' Mean?" on page 19](#)
- > ["Frequently Asked Questions" on page 20](#)

Supported Cryptographic Algorithms

The K7 Cryptographic engine supports cryptographic algorithms that include:

- > RSA
- > DSA
- > Diffie-Hellman
- > DES and triple DES
- > MD2 and MD5
- > SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
- > RC2, RC4 and RC5
- > AES
- > PBE
- > ECC
- > ECIES
- > ARIA, SEED

Included with SafeNet Product Software Development Kit is a sample application – and the source code – to accelerate integration of SafeNet's cryptographic engine into your system.

Application Programming Interface (API) Overview

The major API provided with SafeNet Product Software Development Kit conforms to RSA Laboratories' Public-Key Cryptography Standards #11 (PKCS #11) v2.20, as described in ["PKCS#11 Support" on page 23](#). A set of API services (called PKCS #11 Extensions) designed by SafeNet, augments the services provided by PKCS#11, as described in ["Extensions to PKCS#11" on page 29](#). The extensions to each API enable optimum use of SafeNet hardware for commonly used calls and functions, where the unaugmented API would tend to use software, or to make generic, non-optimized use of available HSMs.

In addition, support is provided for Microsoft's cryptographic APIs (CAPI/CNG) (see ["Microsoft Interfaces" on page 395](#) and Oracle's Java Security API (see ["Java Interfaces" on page 370](#)).

The API is a library – a DLL in Windows, a shared object in Solaris, AIX and Linux – called Chrystoki. Applications wanting to use token services must connect with Chrystoki.

Table 1: SafeNet libraries by platform

Platform	Key name	Libraries
Windows	LibNT	X:\Program Files\SafeNet\LunaClient\cryptoki.dll
		X:\Program Files\SafeNet\LunaClient\cklog201.dll
		X:\Program Files\SafeNet\LunaClient\shim.dll
		X:\Program Files\SafeNet\LunaClient\LunaCSP\LunaCSP.dll
		C:\WINDOWS\system32\SafeNetKSP.dll
Solaris (64-bit)	LibUNIX64	/opt/safenet/lunaclient/lib/libCryptoki2_64.so
		/opt/safenet/lunaclient/lib/libcklog2.so
		/opt/safenet/lunaclient/lib/libshim_64.so
Linux (64-bit)	LibUNIX64	/usr/safenet/lunaclient/lib/libCryptoki2_64.so
		/usr/safenet/lunaclient/lib/libcklog2.so
		/usr/safenet/lunaclient/lib/libshim_64.so
AIX (64-bit)	LibAIX	/usr/safenet/lunaclient/lib/libCryptoki2.so
		/usr/safenet/lunaclient/lib/libCryptoki2_64.so
		/usr/safenet/lunaclient/lib/libcklog2.so
		/usr/safenet/lunaclient/lib/libshim.so

Sample Application

Included with SafeNet Product Software Development Kit is a sample application – and the source code – to accelerate integration of SafeNet's cryptographic engine into your system.

NOTE To reduce development or adaptation time, you may re-distribute the salogin program to customers who use SafeNet Luna PCIe HSM, in accordance with the terms of the End User License Agreement. However, you may not re-distribute the SafeNet Software Development Kit itself.

A Note About RSA Key Attributes 'p' and 'q'

When RSA keys are generated, 'p' and 'q' components are generated which, theoretically, could be of considerably different sizes.

Unwrapping

The SafeNet Luna PCIe HSM allows RSA private keys to be unwrapped onto the HSM where the lengths of the 'p' and 'q' components are unequal. Because the effective strength of an RSA key pair is determined by the length of the shorter component, choosing 'p' and 'q' to be of equal length provides the maximum strength from the generated key pair. If your application is designed to generate key pairs that will be unwrapped onto the HSM, care should be taken in choosing the lengths of the 'p' and 'q' components such that they differ by no more than 15%.

Generation

Where you are generating RSA private keys within the HSM, the HSM enforces that 'p' and 'q' be equal in size, to the byte level.

A Note About the Shim

The Client install includes a shim library to support PKCS#11 integration with various third-party products. You should have no need for this shim library in your development. If for some reason you determine that you need the shim, Chrystoki supports it.

What Does 'Supported' Mean?

With the exception of some generic items that (for example) might need to be set in Windows when installing CSP, KSP, or Java, we do not include a list of integrations in the main product documentation.

Instead, you can check with the <https://supportportal.gemalto.com> website for third-party applications that have been integrated and tested with SafeNet Luna PCIe HSMs by our Integrations group. That group is constantly testing and updating third-party integrations and publishing notes and instructions to help you integrate our HSMs with your applications.

As a general rule, if a specific version of an application and a specific version of a SafeNet Luna PCIe HSM product are mentioned in an Integration document, then those items will definitely work together. A newer version of the SafeNet Luna PCIe HSM or its attendant software is most likely to work with the indicated application without problem. We take care, for several generations of a given HSM product, to not break working relationships, though eventually it might happen that very old versions of third-party software and systems can no longer be supported. One thing that can sometimes happen is that we update HSM firmware to include newer algorithms, and to exclude older algorithms or key sizes that no longer meet industry-accepted standards (like NIST, Common Criteria, etc.).

A newer version of a third-party software might, or might not work with SafeNet Luna PCIe HSMs that were tested to work with a specific earlier version of the same software. This is because some vendors make changes in their products that require new adaptation or at least new configuration instructions. If this happens to you, Thales Customer Support or Sales Engineering is usually happy to work with you to find a solution - both to support you as one of our customers and to have a revised/new integration that can be added to our portfolio.

Check the website or contact Thales Customer Support for the latest list of third-party applications that are tested and supported with SafeNet Luna PCIe HSMs.

Why Is an Integration Not Listed Here Or On the Website?

In many cases, third-party application vendors see a need to integrate their application with Gemalto SafeNet products. In those cases, the third-party company performs the integration and testing, and also provides the support for the integrated solution to their customers (including you). For integrations not listed by Thales, please contact the application vendor for current information.

Similarly some value-added resellers and custom/third-party integrators or consultants might have performed specific integrations of SafeNet Luna PCIe HSMs for the benefit of their specific customers. If you have purchased services or product from such a supplier, you will need to contact them for support of such integrations.

Third-party-tested integrations are not listed here or on the Thales website library of integration documents because we have not verified them in our own labs. If you contact Thales Support regarding use of our product with an application that we have not integrated, you will be asked to contact the third party that performed the integration.

Frequently Asked Questions

This section provides additional information by answering questions that are frequently asked by our customers.

How can we use a SafeNet Luna PCIe HSM with a Key Manager?

A SafeNet Luna PCIe HSM could be a Certificate Authority (CA) within your organization, and would operate in parallel with a Key Manager. It is normally the Key Manager that requests service from a CA, and not the other way around. For example, the Key Manager might generate an RSA key pair for an endpoint to use for authentication. The KM would then go to its associated CA and request a certificate for the public key.

The other typical use case for a KM looking to a CA for service is for confirming certificate validity, either through CRLs or OCSP.

In general, the HSM keeps keys safe within its confines, and exports only metadata about the contained objects. The metadata allows the KM or an integrated application to refer to the keys and objects within the HSM, when invoking cryptographic operations by the HSM, but not to touch the actual keys or objects themselves.

A CA's private key(s) are extremely valuable and often are used only by a CA application operating on a stand-alone server or one on a very minimally-connected subnet. Backup is normally done to a Safenet Luna Backup HSM that can then be locked away in a safe.

We need to encrypt PANs on MS SQL Server 2008 (Extensible Key Management). We have a problem with the encrypted PAN, as the length is greater than the original PAN (16 digits).

The issue is a common one and it arises because the CBC padding scheme requires an extra padding block (8 bytes), with all bytes having the hex value 8, to be appended if the length of the original plaintext is a multiple of the cipher's block length. Another format issue often comes up as well since encrypted data does not generally represent well as decimal digits.

We suggest one of two options:

1. You can set up a shadow table to hold the encrypted PANs. The shadow table schema can then be set up for a sufficient number of hex numerals to hold the padded data or just make that field a binary blob. This takes some coding on your part, and the plaintext PANs would be retrieved into a dynamic view, rather than back into the "real" table, to protect their confidentiality. You should do this only if there is a hard requirement to use SafeNet Luna PCIe HSM, such as certification.
2. Alternatively, you can switch to DataSecure. It has tokenization support and is, in general, designed for DB security.

"Makecert" fails when using SafeNet Luna PCIe HSM with MS Authenticode, because the MD5 algorithm is not available when the HSM is in FIPS mode.

Error: CryptHashPublicKeyInfo failed => 0x80090005 (-2146893819) Failed, and FINIDigest_Init *CKR_MECHANISM_INVALID***(296ms) {}**

The certificate always has an MD5 hash in it. Configure LunaCSP algorithm registration such that MD5 hashing is performed in software. For example:

```
# register.exe /algorithms
```

We are developing our application(s) in C#, and we want to integrate with SafeNet Luna PCIe HSMs

If you want to integrate your C# application with SafeNet Luna PCIe HSM 6.x using PKCS#11 calls, rather than using Microsoft CAPI or CNG, then you might consider using "ncryptoki". At the time this note is being written, we have not created anything formal, but we have worked with some customers who are successfully using "ncryptoki" for that purpose.

Keep an eye on the Safenet C3 website, or ask your SafeNet technical representatives if anything new has been added. Or, you could engage SafeNet Professional Services for formal assistance with your project.

We intend to use PKCS#11 data objects - is this supported in the API for your HSMs?

Yes, it's a basic requirement.

If you have concerns, you might wish to verify if SafeNet Luna PCIe HSMs' (and our API's) handling of data objects are conducive to the operation of your intended application(s). SafeNet API generally places no restrictions on whether data objects can be private or not. We understand that, in the past, some competitors' modules might have allowed only public data objects, if that was the basis of your question.

However, one concern that might arise is Java.

Java offers no support for data objects, and so we do not support them with the LunaProvider. Unexpected results can occur with SafeNet JCA if a data object is present in a partition. This might be the case if you attempt to use an application that uses the CSP, and then the JSP accesses the same partition. CSP inherently creates a data object for its own purposes.

Therefore, keep CSP and JSP clients tied to separate partitions. Generally do not allow JSP to connect to a partition that contains a data object, regardless of the source - Java (and therefore JSP) doesn't know what to do with it.

If your application scenario really does demand the use of both the Microsoft Cryptographic Provider and Java against a common partition, then consider upgrading/updating to Microsoft CNG and use our KSP, which does not inherently create a data object, and so would not cause conflict of that sort.

In our application, both for PKCS#11 and for the JCA/JCE SafeNet Provider, we need to use CKM_SHAxxx_RSA_PKCS mechanism for Signing. Does Hashing occur at the Client or in the HSM?
CKM_SHAxxx_RSA_PKCS is a PKCS#11 mechanism, not a Java method.

For PKCS#11 the digest operation is done within the HSM if that mechanism is called.

For Java, digests are done in software.

We were using another vendor's HSM - or are evaluating HSM products - to host an online sub- or issuing CA with MSCA. With the other vendor we must check "Allow administrator interaction when the private key is accessed by the CA" in the "Configure Cryptography" setup dialog.

SafeNet Luna PCIe HSMs seem to work regardless of whether that selection is checked or not.

So, for that other vendor's product, you need to enter the additional credentials every time you need to issue a certificate? That seems a bit restrictive.

"Allow administrator interaction..." actually means "Allow administrator interaction if the underlying KSP requires it".

The Windows operating system passes a Windows handle that the KSP can use to render any GUI designed by a vendor (SafeNet or some other vendor).

Somewhere in the process a KSP reports that it can (or cannot) interact with the GUI so the application will (or will not) request GUI interaction; that is, pass a window handle to the KSP.

So, the <competitor product> KSP expects a window handle - implying hands-on action by an administrator, each time - whereas SafeNetKsp ignores the handle (if one was provided).

SafeNet's KSP was designed to register partitions ahead of time. SafeNet Luna PCIe HSMs can be Activated, which caches the administrative and enabling credentials, such that only the partition challenge (text string) is needed, which can be passed by your application without need for GUI interaction. Furthermore, SafeNet Luna PCIe HSM can "AutoActivate" partitions, which allows cached ("Activated") partition credentials to be retained through power interruptions as long as 2 hours in duration.

For SafeNet Luna PCIe HSMs, as long as the user is registered in the KSP utility, and the partition is activated, the "Allow administrator interaction..." check box (checked or not checked) does not impose any additional, ongoing, authentication requirements -- no additional prompts for credentials from the GUI. After initial setup and Activation, the SafeNet Luna PCIe HSM knows what to do, and doesn't need to pester you.

For root CAs, on the other hand, you always have the option of not activating the partition, so PED interaction would always be required to ensure close supervision for each use of the private key.

CHAPTER 2: PKCS#11 Support

This chapter describes the PKCS#11 support provided by the SafeNet SDK. It contains the following topics:

- > ["PKCS#11 Compliance" below](#)
- > ["Using the PKCS#11 Sample" on page 27](#)

PKCS#11 Compliance

This section shows the compliance of SafeNet Software Development Kit HSM products to the PKCS#11 standard, with reference to particular versions of the standard. The text of the standard is not reproduced here.

Supported PKCS#11 Services

The table below identifies which PKCS#11 services this version of SafeNet Software Development Kit supports. The table following lists other features of PKCS#11 and identifies the compliance of this version of the SafeNet Software Development Kit to these features.

Table 1: PKCS#11 function support

Category	Function	Supported SafeNet ver 2.20
General purpose functions	C_Initialize	Yes
	C_Finalize	Yes
	C_GetInfo	Yes
	C_GetFunctionList	Yes

Category	Function	Supported SafeNet ver 2.20
Slot and token management functions	C_GetSlotList	Yes
	C_GetSlotInfo	Yes
	C_GetTokenInfo	Yes
	C_WaitForSlotEvent	No
	C_GetMechanismList	Yes
	C_GetMechanismInfo	Yes
	C_InitToken	Yes
	C_InitPIN	Yes
	C_SetPIN	Yes
Session management functions	C_OpenSession	Yes
	C_CloseSession	Yes
	C_CloseAllSessions	Yes
	C_GetSessionInfo	Yes
	C_GetOperationState	Yes
	C_SetOperationState	Yes
	C_Login	Yes
	C_Logout	Yes

Category	Function	Supported SafeNet ver 2.20
Object management functions	C_CreateObject	Yes
	C_CopyObject	Yes
	C_DestroyObject	Yes
	C_GetObjectSize	Yes
	C_GetAttributeValue	Yes
	C_SetAttributeValue	Yes
	C_FindObjectsInit	Yes
	C_FindObjects	Yes
	C_FindObjectsFinal	Yes
Encryption functions	C_EncryptInit	Yes
	C_Encrypt	Yes
	C_EncryptUpdate	Yes
	C_EncryptFinal	Yes
Decryption functions	C_DecryptInit	Yes
	C_Decrypt	Yes
	C_DecryptUpdate	Yes
	C_DecryptFinal	Yes
Message digesting functions	C_DigestInit	Yes
	C_Digest	Yes
	C_DigestUpdate	Yes
	C_DigestKey	Yes
	C_DigestFinal	Yes

Category	Function	Supported SafeNet ver 2.20
Signing and MACing functions	C_SignInit	Yes
	C_Sign	Yes
	C_SignUpdate	Yes
	C_SignFinal	Yes
	C_SignRecoverInit	No
	C_SignRecover	No
Functions for verifying signatures and MACs	C_VerifyInit	Yes
	C_Verify	Yes
	C_VerifyUpdate	Yes
	C_VerifyFinal	Yes
	C_VerifyRecoverInit	No
	C_VerifyRecover	No
Dual-purpose cryptographic functions	C_DigestEncryptUpdate	No
	C_DecryptDigestUpdate	No
	C_SignEncryptUpdate	No
	C_DecryptVerifyUpdate	No
Key management functions	C_GenerateKey	Yes
	C_GenerateKeyPair	Yes
	C_WrapKey	Yes
	C_UnwrapKey*	Yes
	C_DeriveKey	Yes
Random number generation functions	C_SeedRandom	Yes
	C_GenerateRandom	Yes

Category	Function	Supported SafeNet ver 2.20
Parallel function management functions	C_GetFunctionStatus	No
	C_CancelFunction	No
Callback function		No

*C_UnwrapKey has support for the CKA_Unwrap_Template object. All mechanisms which perform the unwrap function support an unwrap template. Nested templates are not supported.

Table 2: PKCS#11 feature support

Feature	Supported?
Exclusive sessions	Yes
Parallel sessions	No

Additional Functions

Please note that certain additional functions have been implemented by SafeNet as extensions to the standard. These include aspects of object cloning, and are described in detail in ["SafeNet Luna Extensions to PKCS#11" on page 29](#).

Using the PKCS#11 Sample

The SafeNet SDK includes a simple "C" language cross platform source example, **p11Sample**, that demonstrates the following:

- > How to dynamically load the SafeNet cryptoki library.
- > How to obtain the function pointers to the exported PKCS11 standard functions and the SafeNet extension functions.

The sample demonstrates how to invoke some, but not all of the API functions.

The SfntLibPath Environment Variable

The sample depends on an environment variable created and exported prior to execution. This variable specifies the location of **cryptoki.dll** (Windows) or **libCryptoki2.so** on Linux/UNIX. The variable is called **SfntLibPath**. You are free to provide your own means for locating the library.

What p11Sample Does

The p11Sample program performs the following actions:

1. The sample first attempts to load the dynamic library in the function called **LoadP11Functions**. This calls **LoadLibrary** (Windows) or **dlopen** (Linux/UNIX).

2. The function then attempts to get a function pointer to the PKCS11 API **C_GetFunctionList** using **GetProcAddress** (Windows) or **dlsym** (Linux/UNIX).
3. Once the function pointer is obtained, use the API to obtain a pointer called **P11Functions** that points to the static CK_FUNCTION_LIST structure in the library. This structure holds pointers to all the other PKCS11 API functions supported by the library.

At this point, if successful, PKCS11 APIs may be invoked like the following:

```
P11Functions->C_Initialize(...);
P11Functions->C_GetSlotList(...);
P11Functions->C_OpenSession(...);
P11Functions->C_Login(...);
P11Functions->C_GenerateKey(...);
P11Functions->C_Encrypt(...);
:
:
etc
```

4. The sample next attempts to get a function pointer to the SafeNet extension API **CA_GetFunctionList** using **GetProcAddress** (Windows) or **dlsym** (Linux/UNIX).
5. Once the function pointer is obtained, use the API to obtain a pointer called **SfntFunctions** that points to the static CK_SFNT_CA_FUNCTION_LIST structure in the library. This structure holds pointers to some but not all of the other SafeNet extension API functions supported by the library.
6. At this point, if successful, SafeNet extension APIs may be invoked like the following:

```
SfntFunctions->CA_GetHState(...);
:
:
etc.
```

7. A sample makefile is provided for 64-bit AIX
You can easily port to another platform with minor changes.
8. To build: `make -f Makefile.aix.64`

NOTE Please note that this simple example loads the cryptoki library directly. If your application requires integration with cklog or ckshim, you will need to load the required library (see SDK General for naming on your platform) in lieu of cryptoki. cklog and ckshim will then use the Chrystoki configuration file to locate and load cryptoki. You also have the option of locating the cryptoki library by parsing the Chrystoki2 section of the Chrystoki config file. If you do this, then the initial library (cryptoki, cklog, or ckshim) can be changed by simply updating the configuration file.

CHAPTER 3: Extensions to PKCS#11

This chapter describes the SafeNet extensions to the PKCS#11 standard. It contains the following topics:

- > "SafeNet Luna Extensions to PKCS#11" below
- > "HSM Configuration Settings" on page 40
- > "Secure PIN Port Authentication" on page 40
- > "High Availability Indirect Login Functions" on page 41
- > "MofN Secret Sharing (quorum or multi-person access control)" on page 44
- > "Key Export Features" on page 44
- > "Derivation of Symmetric Keys with 3DES_ECB" on page 47
- > "PKCS#11 Extension HA Status Call" on page 47
- > "Counter Mode KDF Mechanisms" on page 48
- > "Derive Template" on page 56

SafeNet Luna Extensions to PKCS#11

The following table provides a list of the SafeNet Luna PKCS#11 C-API extensions.

Firmware Dependencies

Some functions are firmware-dependent, as indicated. Where there is a firmware dependency, the specified firmware version applies to all minor revisions of the firmware. In the following table, if no firmware version/series is mentioned, then the extension applies to all. If a firmware version is mentioned, then the extension applies to that firmware series, but not to others. A function that applies to Firmware 4 (example: CA_CloneModifyMofN) works with firmware versions 4.xx.xx, but not with firmware 6.xx.xx nor firmware 7.xx.xx.

Other APIs

These commands and functions can also be used as extensions to other Application Programming Interfaces (for example, OpenSSL).

Cryptoki Version Supported

The current release of SafeNet SafeNet Toolkit provides the Chrystoki library supporting version 2.20 of the Cryptoki standard.

Extension	Description
CA_ActivateMofN	Activates a token that has the secret sharing feature enabled.
CA_CapabilityUpdate	Apply configuration update file as Security Officer only.
CA_CheckOperationState	Checks if the specified cryptographic operation (encrypt, decrypt, sign, verify, digest) is in progress or not in the given session.
CA_CloneAsSource	Refer to the <i>SafeNet Luna Cloning Functions Technical Note</i> , available from Technical Support.
CA_CloneAsTarget	Refer to the <i>SafeNet Luna Cloning Functions Technical Note</i> , available from Technical Support.
CA_CloneAsTargetInit	Refer to the <i>SafeNet Luna Cloning Functions Technical Note</i> , available from Technical Support.
CA_CloneModifyMofN	Firmware 4. Cloning of M of N.
CA_CloneMofN	Firmware 4 cloning of M of N. Copy a cloneable secret-splitting vector from one token to another.
CA_CloneMofN_Common	Firmware 4 cloning of M of N.
CA_CloneObject	Refer to the <i>SafeNet Luna Cloning Functions Technical Note</i> , available from Technical Support.
CA_ClonePrivateKey	Permits the secure transfer a private key (RSA) between a source token and a target token.
CA_CloseApplicationID	Deactivate an application identifier.
CA_CloseApplicationIDForContainer	Deactivate an application identifier for a container.
CA_CloseSecureToken	Firmware 6. Close context for an SFF token.
CA_ConfigureRemotePED	Configure the given slot to use the provided remote PED information (appliance slot only).
CA_CreateContainer	Create a partition for non-PPSO users.
CA_CreateContainerLoginChallenge	Create a challenge for a role on a partition.

Extension	Description
CA_CreateContainerWithPolicy	Firmware 6. Create a partition with per-partition template data.
CA_CreateLoginChallenge	Create a login challenge for the specified user.
CA_Deactivate	Deactivate a partition.
CA_DeactivateMofN	Firmware 4. Deactivate M of N.
CA_DeleteContainer	Delete a partition.
CA_DeleteContainerWithHandle	Delete a partition.
CA_DeleteRemotePEDVector	Delete the Remote PED vector.
CA_DeriveKeyAndWrap	This is an optimization of C_DeriveKey with C_Wrap, merging the two functions into one (the in and out constraints are the same as for the individual functions). A further optimization is applied when mechanism CKM_ECDH1_DERIVE is used with CA_DeriveKeyAndWrap.
CA_DestroyMultipleObjects	Delete multiple objects.
CA_DismantleRemotePED	Inverse of CA_ConfigureRemotePED(). Delete remote PED configuration information.
CA_DuplicateMofN	Create duplicates (copies) of all MofN secret splits.
CA_EncodeECChar2Params	Encode EC curve parameters for user defined curves.
CA_EncodeECPParamsFromFile	Encode EC curve parameters for user defined curves.
CA_EncodeECPrimeParams	Encode EC curve parameters for user defined curves.
CA_Extract	Extract a SIM3 blob.
CA_FactoryReset	Factory Reset the HSM.
CA_FindAdminSlotForSlot	Get the Admin slot for the current slot.
CA_FirmwareRollback	Rollback firmware.
CA_FirmwareUpdate	Firmware 4. Firmware update for Firmware 4 (only used in Luna SA 4.x).

Extension	Description
CA_GenerateCloneableMofN	Create a cloneable secret-splitting vector on a token.
CA_GenerateCloningKEV	Refer to the <i>SafeNet Luna Cloning Functions Technical Note</i> , available from Technical Support.
CA_GenerateMofN	Generate the secret information on a token.
CA_GenerateMofN_Common	Refer to the M of N document.
CA_Get	Get HSM parameters such as serial numbers, and certificates.
CA_GetConfigurationElementDescription	Get capability / policy description and properties.
CA_GetContainerCapabilitySet	Get all partition capability values.
CA_GetContainerCapabilitySetting	Get a single partition capability value.
CA_GetContainerList	Get the list of all partitions on a slot.
CA_GetContainerName	Get the name of a specific partition.
CA_GetContainerPolicySet	Get all partition policy values.
CA_GetContainerPolicySetting	Get a single partition policy value.
CA_GetContainerStatus	Get partition status, which returns authentication status flags.
CA_GetContainerStorageInformation	Get partition storage information such as size, usage, and number of objects.
CA_GetDefaultHSMPolicyValue	Get the default value of a single HSM policy.
CA_GetDefaultPartitionPolicyValue	Get the default value of a single partition policy.
CA_GetFirmwareVersion	Get the vendor-specific firmware version of the SafeNet Luna HSM.
CA_GetHASState	Get HA status from the application perspective.
CA_GetHSMCapabilitySet	Get all HSM capability values.
CA_GetHSMCapabilitySetting	Get a single HSM capability value.

Extension	Description
CA_GetHSMPolicySet	Get all HSM policy values.
CA_GetHSMPolicySetting	Get a single HSM policy value.
CA_GetHSMStats	Get HSM usage stats such as operational counters and how busy the HSM is.
CA_GetHSMStorageInformation	Get HSM storage information such as storage and usage.
CA_GetMofNStatus	Retrieve the MofN structure of the specified token.
CA_GetNumberOfAllowedContainers	Get the number of allowed partitions depending on the partition license count.
CA_GetObjectHandle	Get the object handle for a given OUID.
CA_GetObjectUID	Get the OUID for a given object handle.
CA_GetPartitionPolicyTemplate	Firmware 6. Gets default partition policy template data from HSM.
CA_GetPedId	Get the PED ID.
CA_GetRemotePEDVectorStatus	Get the status of the RPV, created or not.
CA_GetRollbackFirmwareVersion	Get the available rollback version.
CA_GetSecureElementMeta	Get META data for objects on an SFF backup token.
CA_GetServerInstanceBySlotID	Get the instance # in the chrystoki.conf (crystoki.ini) file for the appliance/server the specified slot maps to.
CA_GetSessionInfo	Gets the session info that includes vendor specific information such as authentication state and container handle.
CA_GetSlotIdForContainer	Return a slot for a given container handle.
CA_GetSlotIdForPhysicalSlot	Return a slot for a given physical slot.
CA_GetSlotListFromServerInstance	Get the list of slots for the specified appliance/server instance #, as defined in the chrystoki.conf (crystoki.ini) file.

Extension	Description
CA_GetTime	Get the HSM time.
CA_GetTokenCapabilities	Get the capabilities for the specified partition.
CA_GetTokenCertificateInfo	Get the cloning certificate.
CA_GetTokenCertificates	Get all HSM certificates.
CA_GetTokenInsertionCount	Get the insertion or reset count of HSM in the given slot.
CA_GetTokenObjectHandle	Firmware 6.22.0 or higher. Same as CA_GetObjectHandle for partitions with a partition security officer.
CA_GetTokenObjectUID	Firmware 6.22.0 or higher. Same as CA_GetObjectUID for partitions with a partition security officer.
CA_GetTokenPolicies	Get partition policies.
CA_GetTokenStatus	Get partition status.
CA_GetTokenStorageInformation	Get partition storage information.
CA_GetTunnelSlotNumber	Get the tunnel slot number for a given slot number.
CA_HAActivateMofN	See "High Availability Indirect Login Functions" on page 41 .
CA_HAAnswerLoginChallenge	See "High Availability Indirect Login Functions" on page 41 .
CA_HAAnswerMofNChallenge	See "High Availability Indirect Login Functions" on page 41 .
CA_HAGetLoginChallenge	See "High Availability Indirect Login Functions" on page 41 .
CA_HAGetMasterPublic	See "High Availability Indirect Login Functions" on page 41 .
CA_HAInit	See "High Availability Indirect Login Functions" on page 41 .

Extension	Description
CA_HALogin	See "High Availability Indirect Login Functions" on page 41 .
CA_InitAudit	Initialize the Auditor role.
CA_InitializeRemotePEDVector	Create the Remote PED Vector.
CA_InitRolePIN	Initialize a role on the current slot.
CA_InitSlotRolePIN	Initialize a role on a different slot.
CA_InitToken	Same as CA_Init_token with PPT support.
CA_Insert	Insert a SIM3 blob.
CA_IsMofNEnabled	Firmware 4. Queries M of N status.
CA_IsMofNRequired	Firmware 4. Queries M of N status.
CA_ListSecureTokenInit	Retrieve information from an SFF backup token.
CA_ListSecureTokenUpdate	Continue retrieving information from a backup SFF token.
CA_LogExportSecret	Export (backup) the audit log HMAC key.
CA_LogExternal	Log external message - pushes an application-provided message to the HSM and logs it via the audit log.
CA_LogGetConfig	Get the audit log configuration.
CA_LogGetStatus	Get the audit log status (audit role, logs needing export, HSM to PedClient communication status).
CA_LogImportSecret	Restore the audit log HMAC key.
CA_LogSetConfig	Modify the audit log configuration.
CA_LogVerify	Verify the audit log record(s).
CA_LogVerifyFile	Verify the audit log record file.
CA_ManualKCV	Set the key cloning vector (KCV) (sets the domain).
CA_ModifyMofN	Modify the secret-splitting vector on a token.

Extension	Description
CA_ModifyUsageCount	Modify key usage count (Crypto Officer).
CA_MTKGetState	Firmware 6. Get the master tamper key (MTK) state (tampered or not).
CA_MTKResplit	Generate new MTK split, new purple key value.
CA_MTKRestore	Return MTK, provide purple key to recover from tamper.
CA_MTKSetStorage	Create purple key, enables STM/SRK.
CA_MTKZeroize	Erase the MTK, user invoked tamper. Puts HSM in to transport mode.
CA_OpenApplicationID	Activate an application identifier, independent of any open sessions.
CA_OpenApplicationIDForContainer	Same as CA_OpenApplicationID, but partition specific.
CA_OpenSecureToken	Firmware 6. Open context for an SFF token.
CA_OpenSession	Same as C_OpenSession, but lets you specify partition.
CA_OpenSessionWithAppID	Same as CA_OpenSession, but lets you specify an application ID (AppID)
CA_PerformSelfTest	Invoke a self test on HSM (RNG statistics, Cryptographic Algorithms).
CA_QueryLicense	Get License/CUF information.
CA_ResetDevice	Reset the HSM .
CA_ResetPIN	SO reset of a CO role PIN (if "SO can reset PIN" policy is on).
CA_Restart	Clean up all sessions for a given slot.
CA_RestartForContainer	Clean up all sessions for a given partition.
CA_RetrieveLicenseList	Get a list of all Licenses/CUFs.
CA_RoleStateGet	Get the state of a role (initialized, activated, failed logins, challenge created, etc).

Extension	Description
CA_SetApplicationID	Set the application's identifier.
CA_SetCloningDomain	Set the domain string used during token initialization.
CA_SetContainerPolicies	Set multiple partition policies.
CA_SetContainerPolicy	Set single partition policy.
CA_SetContainerSize	Set container storage size.
CA_SetDestructiveHSMPolicies	Set multiple destructive HSM policies.
CA_SetDestructiveHSMPolicy	Set single destructive HSM policy.
CA_SetHSMPolicies	Set multiple HSM policies.
CA_SetHSMPolicy	Set single HSM policy.
CA_SetKCV	Set KCV (domain).
CA_SetLKCV	Set a legacy KCV (legacy domain).
CA_SetMofN	Set the security policy for the token to use the secret sharing feature.
CA_SetPedId	Set the PED ID for a specific slot.
CA_SetRDK	Set the RDK (role specific KCV) for the current role.
CA_SetTokenPolicies	Set partition policies for given slot (PPSO only)
CA_SetUserContainerName	Set the name the library should use for the user partition on non-PPSO partitions.
CA_SIMExtract	SIM2, SKS, firmware 4.x, firmware 6.x. Extract SIM2 blob.
CA_SIMInsert	SIM2, SKS, firmware 4.x, firmware 6.x. Insert SIM2 blob.
CA_SIMMultiSign	SIM2, SKS, firmware 4.x, firmware 6.x. Sign multiple data blobs with multiple keys provided as SIM2 blobs.
CA_SpRawRead	PED key migration - read PED key value from DataKey PED Key.

Extension	Description
CA_SpRawWrite	PED key migration - store PED key value to iKey PED Key.
CA_STCClearCipherAlgorithm	Remove the specified Cipher Algorithm from use with STC for the specified slot.
CA_STCClearDigestAlgorithm	Remove the specified Digest Algorithm from use with STC for the specified slot.
CA_STCDeregister	Remove STC registration of a client from the specified slot.
CA_STCGetAdminPubKey	Get the public key for the Admin slot's STC identity RSA keypair.
CA_STCGetChannelID	Get the Secure Trusted Channel ID for the current slot.
CA_STCGetCipherAlgorithm	Get all the valid cipher suites allowed for the specified slot.
CA_STCGetCipherID	Get the ID for the cipher currently in use on active STC to this slot.
CA_STCGetCipherIDs	Get all cipher IDs valid for use with STC to the specified slot.
CA_STCGetCipherNameByID	Get the readable name string for the specified Cipher ID.
CA_STCGetClientInfo	Get the STC registration details (name, public key, active access) about the specified client on the specified slot.
CA_STCGetClientsList	Get the list of all STC clients registered to the specified slot.
CA_STCGetCurrentKeyLife	Get the remaining lifetime (in operations) for the active negotiated STC session key.
CA_STCGetDigestAlgorithm	Get all the valid digest algorithms allowed for the specified slot.
CA_STCGetDigestID	Get the ID for the digest currently in use on active STC to this slot.
CA_STCGetDigestIDs	Get all digest IDs valid for use with STC to the specified slot.

Extension	Description
CA_STCGetDigestNameByID	Get the readable name string for the specified Digest ID.
CA_STCGetKeyActivationTimeOut	Get the amount of time allowed between the initiation and completion of STC session negotiation.
CA_STCGetKeyLifeTime	Get the configured session key lifetime (in operations) for the specified slot.
CA_STCGetPartPubKey	Get the public key for the specified slot STC identity RSA keypair.
CA_STCGetPubKey	Get the specified slot's public key.
CA_STCGetSequenceWindowSize	Get the replay window size for the specified slot.
CA_STCGetState	Get the STC state of the specified slot.
CA_STCIsEnabled	Determine if STC is configured for the specified slot.
CA_STCRegister	Register a client for STC to the specified slot.
CA_STCSetCipherAlgorithm	Set a cipher algorithm as valid for use with STC on the specified slot.
CA_STCSetDigestAlgorithm	Set a digest algorithm as valid for use with STC on the specified slot.
CA_STCSetKeyActivationTimeOut	Set the amount of time allowed between the initiation and completion of STC session negotiations for the specified slot.
CA_STCSetKeyLifeTime	Set how long a STC key can live before STC rekeying occurs.
CA_STCSetSequenceWindowSize	Set the replay window size for the specified slot.
CA_STMGetState	Firmware 7. Get STM state (enabled or disabled).
CA_STMToggle	Enter, or recover from, Secure Transport Mode.
CA_TamperClear	Firmware 7. Used by the SO to clear tamper status.
CA_TimeSync	Synchronize the HSM time with the host time.
CA_TokenDelete	SO can delete a partition (PPSO only).

Extension	Description
CA_TokenZeroize	Zeroize a PPSO partition.
CA_ValidateContainerPolicySet	Firmware 7. Validate partition policy settings prior to calling SetPolicies.
CA_ValidateHSMPolicySet	Firmware 7. Validate HSM policy settings prior to calling SetPolicies.
CA_WaitForSlotEvent	For PCMCIA HSMs, extends C_WaitForSlotEvent and provides some history of events.
CA_Zeroize	Zeroize the HSM.

HSM Configuration Settings

SafeNet Luna PCIe HSMs implement configuration settings that can be used to modify the behavior of the HSM, or can be read to determine how the HSM will behave. There are multiple settings that may be manipulated. Other than the "allow non-FIPS algorithms", most customers have no need to either query or change HSM settings. If you believe that your application needs more control over the HSM, please contact SafeNet for guidance.

Secure PIN Port Authentication

Generally, an application collects an authentication code or PIN from a user and/or other source controlled by the host computer. With Gemalto's FIPS 140-2 level 3-validated products (such as SafeNet Luna PCIe HSM), the PIN must come from a device connected to the secure port of the physical interface (or connected via a secure Remote PED protocol connection). The Luna PED (PIN Entry Device) is used for secure entry of PINs.

A bit setting in the device's capabilities settings determines whether the HSM requires that PINs be entered through the secure port. If the appropriate configuration bit is set, PINs must be entered through the secure port.

If the device's configuration bit is off, the application must provide the PIN through the existing mechanism. Through setting the PIN parameters, the application tells the token where to look for PINs. A similar programming approach applies to define the key cloning domain identifier.

Applications wanting PINs to be collected via the secure port must pass a NULL pointer for the pPin parameter and a value of zero for the ulPinLen parameter in function calls with PIN parameters. This restriction applies everywhere PINs are used. The following functions are affected:

- > C_InitToken
- > C_InitIndirectToken
- > C_InitPIN
- > C_SetPIN
- > CA_InitIndirectPIN

- > C_Login
- > CA_IndirectLogin

When domains are generated/collected through the secure port during a C_InitToken call, the application must pass a NULL pointer for the pbDomainString parameter and a value of zero for the ulDomainStringLength parameter in the CA_SetCloningDomain function.

High Availability Indirect Login Functions

NOTE In order to implement High Availability Recovery, the primary and secondary tokens must exist on separate systems.

The following enhancements securely extend the indirect login capability to SafeNet CA3 tokens. SafeNet CA3 tokens to store sensitive information (encrypted) in flash memory, and must therefore be protected against attack by a man-in-the-middle who physically attacks the target token to expose the contents of flash memory, and employs that information against intercepted (or spuriously-generated) message traffic.

The SafeNet CA3 to SafeNet CA3 indirect login protocol also supports old-style MofN authentication between tokens that share an MofN secret.

Initialization functions

Initialization of tokens in a high-availability environment involves three steps:

1. The generation of an RSA login key pair (the public key of the pair may be discarded),
2. Cloning of the private key member to the User (and optionally to the SO) spaces of all tokens within that environment and,
3. Calling the **CA_HAInit** function on all tokens within that environment, in the context of the session owned by the User or SO.

The first two steps are performed using ordinary key generate and cloning Cryptoki function calls. The **CA_HAInit** function is implemented as follows:

CA_HAInit()

```
CK_RV CK_ENTRY CA_HAInit(
CK_SESSION_HANDLE hSession, // Logged-in session of user
// who owns the Login key pair
CK_OBJECT_HANDLE hLoginPrivateKey // Handle to Login private key
);
```

Recovery Functions

The HA recovery mechanism requires the following commands and interface functions:

CA_HAGetMasterPublic()

Called on the primary token, CA_HAGetMasterPublic() retrieves the primary token's TWC (Token Wrapping Certificate) and returns it as a blob (octet string and length). The format of this function is as follows:

```

CK_RV CK_ENTRY CA_HAGetMasterPublic(
CK_SLOT_ID slotId, // Slot number of the primary
// token
CK_BYTE_PTR pCertificate, // pointer to buffer to hold
//TWC certificate
CK_ULONG_PTR pulCertificateLen // pointer to value to hold
//TWC certificate length
);

```

CA_HAGetLoginChallenge()

Called on the secondary token, **CA_HAGetLoginChallenge()** accepts the TWC blob and returns the secondary token's login challenge blob. The format of this command is as follows:

```

CK_RV CK_ENTRY CA_HAGetLoginChallenge(
CK_SESSION_HANDLE hSession, // Public session
CK_USER_TYPE userType, // User type - SO or USER
CK_BYTE_PTR pCertificate, // TWC certificate retrieved
// from primary
CK_ULONG ulCertificateLen, // TWC certificate length
CK_BYTE_PTR pChallengeBlob, // pointer to buffer to hold
// challenge blob
CK_ULONG_PTR pulChallengeBlobLen // pointer to value to hold
// challenge blob length
);

```

CA_HAAnswerLoginChallenge()

Called on the primary token, **CA_HAAnswerLoginChallenge()** accepts the login challenge blob and returns the encrypted SO or User PIN, as appropriate.

```

CK_RV CK_ENTRY CA_HAAnswerLoginChallenge(
CK_SESSION_HANDLE hSession, // Session of the Login Private
// key owner
CK_OBJECT_HANDLE hLoginPrivateKey, // object handle to login key
CK_BYTE_PTR pChallengeBlob, // pointer to buffer containing
// challenge blob
CK_ULONG ulChallengeBlobLen, // length of challenge blob
CK_BYTE_PTR pEncryptedPin, // pointer to buffer holding
// encrypted PIN
CK_ULONG_PTR pulEncryptedPinLen // pointer to value holding
// encrypted PIN length
);

```

CA_HALogin()

Called on the secondary token, **CA_HALogin()** accepts the encrypted PIN and logs the secondary token in. If the second-ary token requires MofN authentication, an MofN challenge blob is returned. If no MofN authentication is required, a zero-length blob is returned. The format of this function is as follows:

```

CK_RV CK_ENTRY CA_HALogin(
CK_SESSION_HANDLE hSession, // Same public session opened
// in CA_HAGetLoginChallenge,
//above
CK_BYTE_PTR pEncryptedPin, // pointer to buffer holding
// encrypted PIN
CK_ULONG ulEncryptedPinLen, // length of encrypted PIN
CK_BYTE_PTR pMofNBlob, // pointer to buffer to hold
// MofN blob

```

```
CK_ULONG_PTR pulMofNBlobLen // pointer to value to hold the
// length of MofN blob
);
```

If the call is successful, then the session now becomes a private session owned by the User or SO (as appropriate).

CA_AnswerMofNChallenge()

Called on the primary token, **CA_AnswerMofNChallenge()** accepts the MofN challenge blob and returns the primary token's masked MofN secret. The format of this function is as follows:

```
CK_RV CK_ENTRY CA_HAAnswerMofNChallenge(
CK_SESSION_HANDLE hSession, // Private session
CK_BYTE_PTR pMofNBlob, // passed in MofN blob
CK_ULONG ulMofNBlobLen, // length of MofN blob
CK_BYTE_PTR pMofNSecretBlob, // pointer to buffer to hold
// MofN secret blob
CK_ULONG_PTR pulMofNSecretBlobLen//pointer to value that holds
// the MofN secret blob len
);
```

CA_HAActivateMofN()

Called on the secondary token, **CA_HAActivateMofN()** accepts the masked MofN secret and performs MofN authentication. The resulting MofN secret is checked against the CRC stored in the MofN PARAM structure.

```
CK_RV CK_ENTRY CA_HAActivateMofN(
CK_SESSION_HANDLE hSession, // The now-private session from
// successful CA_HALogin call
CK_BYTE_PTR pMofNSecretBlob, // pointer to MofN secret
// blob that is passed in
CK_ULONG ulMofNSecretBlobLen // length of MofN secret blob
);
```

It is expected that the recovery functions will be executed in the proper sequence and as part of an atomic operation. Nonetheless, the recovery operation may be restarted at any time due to an error. Restarting the recovery operation resets the state condition of the secondary token, and any data that has been stored or generated on the token is discarded.

Login Key Attributes

The login keys must possess the following attributes to function properly in a HA recovery scenario:

```
// Object
CKA_CLASS = CKO_PRIVATE_KEY,
// StorageClass
CKA_TOKEN = True,
CKA_PRIVATE = True,
CKA_MODIFIABLE = False,
// Key
CKA_KEY_TYPE = CKK_RSA,
CKA_DERIVE = False,
CKA_LOCAL = True,
// Private
CKA_SENSITIVE = True,
CKA_DECRYPT = False,
CKA_SIGN = False,
```

```
CKA_SIGN_RECOVER = False,  
CKA_UNWRAP = False,  
CKA_EXTRACTABLE = False
```

Control of HA Functionality

Refer to for the mechanisms by which the SO can control availability of the HA functionality.

MofN Secret Sharing (quorum or multi-person access control)

In previous SafeNet Luna PCIe HSM releases, this page described library and firmware aspects of MofN secret sharing.

Current implementation (since HSM firmware 5) no longer implements MofN via the HSM.

Instead, MofN is entirely mediated via Luna PED 2.4 and later. The HSM is unaware of secret sharing. Multi-person access control for any of the authentication secrets (SO, User, Cloning domains, Remote PED Vector) is a PED function, and the HSM sees only the fully reconstituted MofN secrets as they are presented to it by the PED.

This implementation is both cleaner and more flexible than the legacy implementation. If you have used, or are still using legacy SafeNet Luna PCIe HSMs, be aware that the legacy implementation of MofN split-secret, multi-person access control is not compatible with the modern implementation. For migration instructions, contact Gemalto Technical Support.

Key Export Features

The SafeNet Key Export HSM provides the feature(s) detailed in this section.

RSA Key Component Wrapping

The RSA Key Component Wrapping is a feature that allows an application to wrap any subset of attributes from an RSA private key with 3-DES. Access to the feature is through the PKCS #11 function `C_WrapKey` with the `CKM_DES3_ECB` mechanism. The wrapping key must be a `CKK_DES2` or `CKK_DES3` key with its `CKA_WRAP` attribute set to `TRUE`. The key to wrap must be an RSA private key with `CKA_EXTRACTABLE` set to `TRUE` and the FPV must have `FPV_WRAPPING_TOKEN` turned on.

The details of the wrapping format are specified with a format descriptor. The format descriptor is provided as the mechanism parameter to the `CKM_DES3_ECB` mechanism. This descriptor consists of a 32-bit format version, followed by a set of field element descriptors. Each field element descriptor consists of a 32-bit Field Type Identifier and optionally some additional data. The SafeNet firmware parses the set of field element descriptors and builds the custom layout of the RSA private key in an internal buffer. Once all field element descriptors are processed, the buffer is wrapped with 3-DES and passed out to the calling application. It is the responsibility of the calling application to ensure that the buffer is a multiple of 8 bytes.

The format descriptor version (the first 32-bit value in the format data) must always be set to zero.

The set of supported field element descriptor constants is as follows:

- > `#define KM_APPEND_STRING 0x00000000`
- > `#define KM_APPEND_ATTRIBUTE 0x00000001`

- > #define KM_APPEND_REVERSED_ATTRIBUTE 0x00000002
- > #define KM_APPEND_RFC1423_PADDING 0x00000010
- > #define KM_APPEND_ZERO_PADDING 0x00000011
- > #define KM_APPEND_ZERO_WORD_PADDING 0x00000012
- > #define KM_APPEND_INV_XOR_CHECKSUM 0x00000020
- > #define KM_DEFINE_IV_FOR_CBC 0x00000030

The meanings of the field element descriptors is as follows:

Field element descriptor	Description
KM_APPEND_STRING	<p>Appends an arbitrary string of bytes to the custom layout buffer.</p> <p>The field type identifier is followed by a 32-bit length field defining the number of bytes to append. The length field is followed by the bytes to append.</p> <p>There is no restriction of the length of data that may be appended, as long as the total buffer length does not exceed 3072 bytes.</p>
KM_APPEND_ATTRIBUTE	<p>Appends an RSA private key component into the buffer in big endian representation.</p> <p>The field type identifier is followed by a 32-bit CK_ATTRIBUTE_TYPE value set to one of the following: CKA_PRIVATE_EXPONENT, CKA_PRIME_1, CKA_PRIME_2, CKA_EXPONENT_1, CKA_EXPONENT_2, or CKA_COEFFICIENT..</p> <p>The key component is padded with leading zeros such that the length is equal to the modulus length in the case of the private exponent, or equal to half of the modulus length in the case of the other 5 components.</p>
KM_APPEND_REVERSED_ATTRIBUTE	<p>Appends an RSA private key component into the buffer in little endian representation.</p> <p>The field type identifier is followed by a 32-bit CK_ATTRIBUTE_TYPE value set to one of the following: CKA_PRIVATE_EXPONENT, CKA_PRIME_1, CKA_PRIME_2, CKA_EXPONENT_1, CKA_EXPONENT_2, or CKA_COEFFICIENT.</p> <p>The key component is padded with trailing zeros such that the length is equal to the modulus length in the case of the private exponent, or equal to half of the modulus length in the case of the other 5 components.</p>
KM_APPEND_RFC1423_PADDING	<p>Applies RFC 1423 padding to the buffer (appends 1 to 8 bytes with values equal to the number of bytes, such that the total buffer length becomes a multiple of 8).</p> <p>This would typically be the last formatting element in a set, but this is not enforced.</p>
KM_APPEND_ZERO_PADDING	<p>Applies Zero padding to the buffer (appends 0 to 7 bytes with values equal to Zero, such that the total buffer length becomes a multiple of 8).</p> <p>This would typically be the last formatting element in a set, but this is not enforced.</p>
KM_APPEND_ZERO_WORD_PADDING	<p>Zero pads the buffer to the next 32-bit word boundary.</p>

Field element descriptor	Description
KM_APPEND_INV_XOR_CHECKSUM	Calculates and adds a checksum byte to the buffer. The checksum is calculated as the complement of the bitwise XOR of the buffer being built.
KM_DEFINE_IV_FOR_CBC	Allows definition of an IV so that 3DES_CBC wrapping can be performed even though the functionality is invoked with the CKM_3DES_ECB mechanism. The field type identifier is followed by a 32-bit length field, which must be set to 8. The length is followed by exactly 8 bytes of data which are used as the IV for the wrapping operation.

Examples

To wrap just the private exponent of an RSA key in big endian representation, the parameters would appear as follows:

NOTE Ensure that the packing alignment for your structures uses one (1) byte boundaries.

```
struct
{
  UInt32 version = 0;
  UInt32 elementType = KM_APPEND_ATTRIBUTE;
  CK_ATTRIBUTE_TYPE attribute = CKA_PRIVATE_EXPONENT;
}
```

To wrap the set of RSA key components Prime1, Prime2, Coefficient, Exponent1, Exponent2 in little endian representation with a leading byte of 0x05 and ending with a CRC byte and then zero padding, the parameters would appear in a packed structure as follows:

```
struct
{
  UInt32 version = 0;
  UInt32 elementType1 = KM_APPEND_STRING;
  UInt32 length = 1;
  UInt8 byteValue = 5;
  UInt32 elementType2 = KM_APPEND_REVERSED_ATTRIBUTE;
  CK_ATTRIBUTE_TYPE attribute1 = CKA_PRIME_1;
  UInt32 elementType3 = KM_APPEND_REVERSED_ATTRIBUTE;
  CK_ATTRIBUTE_TYPE attribute2 = CKA_PRIME_2;
  UInt32 elementType4 = KM_APPEND_REVERSED_ATTRIBUTE;
  CK_ATTRIBUTE_TYPE attribute3 = CKA_COEFFICIENT;
  UInt32 elementType5 = KM_APPEND_REVERSED_ATTRIBUTE;
  CK_ATTRIBUTE_TYPE attribute4 = CKA_EXPONENT_1;
  UInt32 elementType6 = KM_APPEND_REVERSED_ATTRIBUTE;
  CK_ATTRIBUTE_TYPE attribute5 = CKA_EXPONENT_2;
  UInt32 elementType7 = KM_APPEND_INV_XOR_CHECKSUM;
  UInt32 elementType8 = KM_APPEND_ZERO_PADDING;
}
```

Derivation of Symmetric Keys with 3DES_ECB

SafeNet supports derivation of symmetric keys by the encryption of "diversification data" with a base key. Access to the derivation functionality is through the PKCS#11 C_DeriveKey function with the CKM_DES3_ECB and CKM_DES_ECB mechanism. Diversification data is provided as the mechanism parameter. The derived key can be any type of symmetric key. The encrypted data forms the CKA_VALUE attribute of the derived key. A template provided as a parameter to the C_DeriveKey function defines all other attributes.

Rules for the derivation are as follows:

- > The Base Key must be of type CKK_DES2 or CKK_DES3 when using CKM_DES3_ECB. It must be of type CKK_DES when using CKM_DES_ECB.
- > The base key must have its CKA_DERIVE attribute set to TRUE.
- > The template for the derived key must identify the key type (CKA_KEY_TYPE) and length (CKA_VALUE_LEN). The type and length must be compatible. The length can be omitted if the key type supports only one length. (E.g., If key type is CKK_DES2, the length must either be explicitly defined as 16, or be omitted to allow the value to default to 16). Other attributes in the template must be consistent with the security policy settings of the SafeNet Luna PCIe HSM.
- > The derivation mechanism must be set to CKM_DES3_ECB or CKM_DES_ECB, the mechanism parameter pointer must point to the diversification data, and the mechanism parameter length must be set to the diversification data length.
- > The diversification data must be the same length as the key to be derived, with one exception. If the key to be derived is 16 bytes, the base key is CKK_DES2 and the diversification data is only 8 bytes, then the data is encrypted twice - once with the base key and once with the base key with its halves reversed. Joining the two encrypted pieces forms the derived key.
- > If the derived key is of type CKK_DES, CKK_DES2 or CKK_DES3, odd key parity is applied to the new key value immediately following the encryption of the diversification data. The encrypted data is taken as-is for the formation of all other types of symmetric keys.

PKCS#11 Extension HA Status Call

A SafeNet extension to the PKCS#11 standard allows query of the HA group state.

Function Definition

```
CK_RV CK_ENTRY CA_GethASState( CK_SLOT_ID slotId, CK_HA_STATE_PTR pState );
```

The structure definitions for a CK_HA_STATE_PTR and CK_HA_MEMBER are:

```
typedef struct CK_HA_MEMBER{
CK_ULONG memberSerial;
CK_RV memberStatus;
}CK_HA_MEMBER;
```

```
typedef struct CK_HA_STATUS{
CK_ULONG groupSerial;
CK_HA_MEMBER memberList[CK_HA_MAX_MEMBERS];
CK_USHORT listSize;
}CK_HA_STATUS;
```

See the JavaDocs included with the software for a description of the Java methods derived from this cryptoki function.

Counter Mode KDF Mechanisms

The SafeNet Luna PCIe HSMs support the following two vendor defined mechanisms. They can be used to perform Counter Mode KDF (key derivation functions) using various CMAC algorithms (DES3, AES, ARIA, SEED) as the PRF (pseudo-random function). See NIST SP 800-108.

```
#define CKM_NIST_PRF_KDF                (CKM_VENDOR_DEFINED + 0xA02)
#define CKM_PRF_KDF                    (CKM_VENDOR_DEFINED + 0xA03)

/* Parameter and values used with CKM_PRF_KDF and * CKM_NIST_PRF_KDF. */

typedef CK_ULONG CK_KDF_PRF_TYPE;
typedef CK_ULONG CK_KDF_PRF_ENCODING_SCHEME;

/** PRF KDF types */
#define CK_NIST_PRF_KDF_DES3_CMAC      0x00000001
#define CK_NIST_PRF_KDF_AES_CMAC      0x00000002
#define CK_PRF_KDF_ARIA_CMAC          0x00000003
#define CK_PRF_KDF_SEED_CMAC          0x00000004

#define LUNA_PRF_KDF_ENCODING_SCHEME_1 0x00000000
#define LUNA_PRF_KDF_ENCODING_SCHEME_2 0x00000001

typedef struct CK_KDF_PRF_PARAMS {
    CK_KDF_PRF_TYPE      prfType;
    CK_BYTE_PTR          pLabel;
    CK_ULONG              ulLabelLen;
    CK_BYTE_PTR          pContext;
    CK_ULONG              ulContextLen;
    CK_ULONG              ulCounter;
    CK_KDF_PRF_ENCODING_SCHEME ulEncodingScheme;
} CK_PRF_KDF_PARAMS;

typedef CK_PRF_KDF_PARAMS CK_PTR CK_KDF_PRF_PARAMS_PTR;
```

BIP32 Mechanism Support and Implementation

This section describes the BIP32 functions, key attributes, error codes, and mechanisms supported for BIP32 with the HSM.

Curve Support

Only curve secp256k1 is supported. The BIP32 derivation mechanisms fail with CKR_TEMPLATE_INCONSISTENT if you attempt to specify a curve with CKA_ECDSA_PARAMS.

Key Type and Form

The key type `CKK_BIP32` is used to distinguish keys that can be used for BIP32 from all the existing ECDSA keys. Existing ECDSA keys cannot be used with any of the BIP32 mechanisms because they lack a chain code. The serialization format when importing, exporting, wrapping and unwrapping keys is also different from ECDSA keys. All mechanisms supported by ECDSA keys are supported for BIP32 keys.

Extended Keys and Hardened Keys

BIP32 includes hardened and non-hardened (normal) child keys. Each has a 32-bit index. Child keys are considered hardened if the most significant bit of their index is set. This bit is defined as `CKF_BIP32_HARDENED`. This allows 2^{31} hardened keys and 2^{31} non-hardened keys per parent.

Hardened private keys create a firewall through which multi-level key derivation compromises cannot happen. For normal (non-hardened) keys one can derive child public keys of a given parent key without knowing any private key. So if an attacker gets a normal parent chain code and parent public key, he can brute-force all chain codes deriving from it. If the attacker also obtains a child, grandchild, or further-descended private key, he can use the chain code to generate all of the extended private keys descending from that private key. The formula for creating hardened keys makes it impossible to create child public keys without knowing the parent private key.

Key Derivation

Two new mechanisms are added to support all the key derivations in BIP32.

CKM_BIP32_MASTER_DERIVE

This mechanism derives the master key pair from a seed. The input key must have the type `CKK_GENERIC_SECRET` (size between 128 and 512 bits). This mechanism is unique in that it derives two keys from one. This requires us to accept two templates as input, and to output the two derived key handles. In order to avoid confusion, the three last arguments of `C_DeriveKey()` (`pTemplate`, `ulAttributeCount` and `phKey`) must be null or zero. `CKR_ARGUMENTS_BAD` is returned if any of those parameters is non-NULL. The templates and returned handles are instead passed in through the mechanism parameters, which are clearly labeled public and private. Choose to not generate the public or private key by leaving those parameters as zero or null.

```
typedef struct CK_BIP32_MASTER_DERIVE_PARAMS {
    CK_ATTRIBUTE_PTR pPublicKeyTemplate;
    CK_ULONG ulPublicKeyAttributeCount;
    CK_ATTRIBUTE_PTR pPrivateKeyTemplate;
    CK_ULONG ulPrivateKeyAttributeCount;
    CK_OBJECT_HANDLE hPublicKey; // output parameter
    CK_OBJECT_HANDLE hPrivateKey; // output parameter
} CK_BIP32_MASTER_DERIVE_PARAMS;
```

See ["Code Samples" on page 53](#) for a code example.

CKM_BIP32_CHILD_DERIVE

This mechanism derives child keys from a parent key. The mechanism can generate both the private and public part of the key pair, and can accept a BIP32 public or private key as input. An error is returned if a public to private derivation is attempted. Like the master key derivation, the templates and key handle outputs are passed through the mechanism parameters. Choose to not generate the public or private key by leaving those parameters as zero or null.

The BIP32 and BIP44 specifications recommend wallet structures and use cases. The specifications provide a good reference for deciding how a key tree should be organized and if a particular key should be hardened or not. Follow the specifications to avoid potential security holes.

This mechanism can be used to generate keys that are several levels deep in the key hierarchy. The path of the key is specified with `pulPath` and `ulPathLen`. The path is an array of integers (key indices). The path is relative to the input key. For example, if the path is [5, 1, 4] and the path of the input key is m/0 then the resulting path is m/0/5/1/4.

```
typedef struct CK_BIP32_CHILD_DERIVE_PARAMS {
    CK_ATTRIBUTE_PTR pPublicKeyTemplate;
    CK_ULONG ulPublicKeyAttributeCount;
    CK_ATTRIBUTE_PTR pPrivateKeyTemplate;
    CK_ULONG ulPrivateKeyAttributeCount;
    CK_ULONG_PTR pulPath;
    CK_ULONG ulPathLen;
    CK_OBJECT_HANDLE hPublicKey; // output parameter
    CK_OBJECT_HANDLE hPrivateKey; // output parameter
    CK_ULONG ulPathErrorIndex; // output parameter
} CK_BIP32_CHILD_DERIVE_PARAMS;
```

See ["Code Samples" on page 53](#) for a code example.

Error Codes

These mechanisms can fail in ways not applicable to other mechanisms.

CKR_BIP32_CHILD_INDEX_INVALID: This error is returned on the rare occurrence ($1 / 2^{127}$) that a child derivation returns an all-zero private key, a private key bigger than or equal to the curve order parameter n , or a point at infinity. This error signifies that the child key index cannot be used to derive keys. Choose a different index and try the derivation again. The problematic child index is indicated by `ulPathErrorIndex`.

PKCS#11 does not have fixed width integers. This error can also be returned on platforms where `CK_ULONG` is bigger than 32 bits and a child index is bigger than $2^{32} - 1$.

CKR_BIP32_INVALID_HARDENED_DERIVATION: This error is returned from an attempt to derive a hardened key from a public key. The BIP32 specification does not support such a derivation.

CKR_BIP32_MASTER_SEED_LEN_INVALID: The BIP32 specification recommends deriving the master key from a seed that is between 128 and 512 bits long. This error is returned if the seed length is outside of that range.

CKR_BIP32_MASTER_SEED_INVALID: This error is returned on the rare occurrence ($1 / 2^{127}$) that the master derivation returns an all zero private key, a private key bigger than or equal to the curve order parameter n , or a point at infinity. This error signifies that the master seed cannot be used for BIP32. Generate a new master seed and retry the derivation.

CKR_BIP32_INVALID_KEY_PATH_LEN: This error is returned when `ulPathLen` is 0 or greater than 255. The BIP44 standard only requires paths of length 5 so this limit should be acceptable for all customers.

Key Attributes

The following attributes will exist on all keys created with one of the above derivation mechanisms.

CKA_BIP32_CHAIN_CODE: The chain code is essential for BIP32 keys and is used to derive future keys. The public and private key share this value. Read only.

CKA_BIP32_VERSION_BYTES: Version bytes are used to further identify BIP32 keys. The version bytes help determine if a key is used on the main bitcoin network or the test network. This attribute defaults to `CKG_BIP32_VERSION_MAINNET_PUB/PRIV` if it was not specified at key creation time. You can set this value to `CKG_BIP32_VERSION_TESTNET_PUB/PRIV` if applicable.

CKA_BIP32_CHILD_INDEX: The child index stores which index was used to derive this key. An index with the `CKF_BIP32_HARDENED` bit set is considered a hardened child. The child index is 0 for the master key. The public and private key share this value. Read only.

CKA_BIP32_CHILD_DEPTH: The depth of the child key in the key tree. The master key has a depth of 0. The public and private key share this value. Read only.

CKA_BIP32_ID: The unique identifier for the key. This value is derived from the HASH160 of the compressed public key. The first 32 bits of this value is known as the fingerprint. (`CKA_ID` is not used for this purpose because it is writable by the user.) The public and private key share this value. Read only.

NOTE No attribute is included for the parent ID because it should not be required. The anticipated use-case is to derive a key, use it and then delete it. In general, there should not be a need to discover how keys are organized based on the fingerprints or IDs. The parent fingerprint is available in case there is need to rediscover a key tree, but the wallet software must deal with any collisions. The BIP32 designers considered the parent ID not sufficiently important to include in serialized keys; therefore we exclude it as well.

CKA_BIP32_FINGERPRINT and **CKA_BIP32_PARENT_FINGERPRINT:**

The fingerprints for the key and parent key are the first 32 bits of the BIP32 key identifier. These can be used to identify keys but the wallet software must handle any collisions. For identifying keys, it is better to use **CKA_BIP32_ID** because it is long enough that collisions should not be an issue. The public and private key share this value. The master key has a parent fingerprint of 0. Read only.

Public Key Import/Export

To support importing existing BIP32 keys, we support their serialization format. For public keys, we will have functions in our library to facilitate importing and exporting.

```
CK_RV CA_Bip32ImportPubKey(
    CK_SESSION_HANDLE hSession,
    CK_ATTRIBUTE_PTR pTemplate,
    CK_ULONG ulCount,
    const CK_CHAR_PTR pKey,           //in BIP32 serialization format
    CK_OBJECT_HANDLE_PTR phObject
);
CK_RV CA_Bip32ExportPubKey(
    CK_SESSION_HANDLE hSession,
    CK_OBJECT_HANDLE hObject,
    CK_CHAR_PTR pKey,                 //in BIP32 serialization format
    CK_ULONG_PTR pulKeyLen           //on input contains max. buffer size, returns
                                     // actual size
);
```

Importing is done with `CA_Bip32ImportPubKey()`. The function is similar to `C_CreateObject()` but it takes an additional parameter for the serialized public key. The template passed in should contain all the

desired non-BIP32 attributes like `CKA_TOKEN`, `CKA_PRIVATE`, `CKA_DERIVE`, etc. The function decodes the public key to get all the BIP32 attributes. Both sets of attributes are then used to create the public key on the HSM.

NOTE When importing a serialized extended public key, implementations must verify whether the X coordinate in the public key data corresponds to a point on the curve. If not, the extended public key is invalid.

Exporting is done with `CA_Bip32ExportPubKey()`. The specified object is extracted from the HSM and encoded in the BIP32 format. The result is a NULL-terminated string and is placed in the `pKey` parameter. The length of `pKey` has a maximum of 112 characters. This constant is defined as `CKG_BIP32_MAX_SERIALIZED_LEN`. It's possible that not all characters are needed to serialize the key. Any unused characters are set to 0.

See ["Code Samples" on the next page](#) for code examples.

BIP32 Serialization Format

Extended public and private keys are serialized as follows:

- > 4 byte: version bytes (mainnet: 0x0488B21E public, 0x0488ADE4 private; testnet: 0x043587CF public, 0x04358394 private)
- > 1 byte: depth: 0x00 for master nodes, 0x01 for level-1 derived keys,
- > 4 bytes: the fingerprint of the parent's key (0x00000000 if master key)
- > 4 bytes: child number (index) – 32-bit unsigned integer with most significant byte first (0x00000000 if master key)
- > 32 bytes: the chain code
- > 33 bytes: the public key or private key data

This 78 byte structure is encoded like other Bitcoin data in Base58, by first adding 32 checksum bits (derived from the double SHA-256 checksum), and then converting to the Base58 representation. This results in a Base58-encoded string of up to `CKG_BIP32_MAX_SERIALIZED_LEN` characters. Because of the choice of the version bytes, the Base58 representation will start with "xprv" or "xpub" on mainnet, "tprv" or "tpub" on testnet.

Private Key Import/Export

Private keys can be imported and exported with existing PKCS#11 functions. They can be imported and exported only if the HSM uses the key wrap model instead of cloning. Import a key by calling `C_Encrypt*()` on the serialized key followed by `C_UnwrapKey()`. Exporting keys by calling `C_WrapKey()` followed by `C_Decrypt*()`. Use `C_WrapKey()` and `C_UnwrapKey()` to store keys off the HSM, or to move them between HSMs.

See ["Code Samples" on the next page](#) for code examples.

Key Backup and Cloning

Backups and cloning of BIP32 keys are supported only between version 7.x Luna HSMs. Further, cloning of BIP32 keys is supported only in firmware versions that have BIP32 support. BIP32 keys cannot be cloned to older firmware versions made before BIP32 support was added.

Non-FIPS Algorithm

The BIP32 mechanisms are available only if non-FIPS algorithms are allowed.

Host Tools

Multitoken and Ckdemo support BIP32.

Code Samples

Deriving the master key pair

We highly recommend setting `CKA_PRIVATE` on the master public and private keys to `TRUE` to prevent the chain code from being seen by unauthorized users. The master key should be used only for derivations so it is the only operation allowed. The version bytes default to `0x0488B21E/0x0488ADE4` for the public/private keys if the attribute is missing in the template. Those are the values specified in BIP32 for keys on the main bitcoin network.

```
CK_ATTRIBUTE pubTemplate[] =
{
    {CKA_TOKEN,          &bToken,      sizeof(bToken)},
    {CKA_PRIVATE,       &bTrue,       sizeof(bTrue)},
    {CKA_DERIVE,        &bTrue,       sizeof(bTrue)},
    {CKA_MODIFIABLE,    &bTrue,       sizeof(bTrue)},
    {CKA_LABEL,         pbLabel,      strlen(pbLabel)},
};
CK_ATTRIBUTE privTemplate[] =
{
    {CKA_TOKEN,          &bToken,      sizeof(bToken)},
    {CKA_PRIVATE,       &bTrue,       sizeof(bTrue)},
    {CKA_SENSITIVE,     &bTrue,       sizeof(bTrue)},
    {CKA_DERIVE,        &bTrue,       sizeof(bTrue)},
    {CKA_MODIFIABLE,    &bTrue,       sizeof(bTrue)},
    {CKA_LABEL,         pbLabel,      strlen(pbLabel)},
};

CK_BIP32_MASTER_DERIVE_PARAMS mechParams;
mechParams.pPublicKeyTemplate = pubTemplate;
mechParams.ulPublicKeyAttributeCount = ARRAY_SIZE(pubTemplate);
mechParams.pPrivateKeyTemplate = privTemplate;
mechParams.ulPrivateKeyAttributeCount = ARRAY_SIZE(privTemplate);
CK_MECHANISM mechanism = {CKM_BIP32_MASTER_DERIVE, &mechParams, sizeof(mechParams)};

CK_RV rv = C_DeriveKey(hSession, &mechanism, hSeedKey, NULL, 0, NULL);
// fail if rv != CKR_OK

CK_OBJECT_HANDLE pubKey = mechanism.hPublicKey;
CK_OBJECT_HANDLE privKey = mechanism.hPrivateKey;
```

The new key handles will be stored in `pubKey` and `privKey` if the derivation was successful.

Deriving a child leaf key

We highly recommend setting `CKA_PRIVATE` on the child public and private keys to `TRUE` to prevent the chain code from being seen by unauthorized users. A child leaf key (the bottom key in the tree) should not be used for derivation, and is meant for signing, verifying, encrypting and decrypting. Parent child keys need the derive attribute turned on. The version bytes default to `0x0488B21E/0x0488ADE4` for the public/private keys if the attribute is missing. Those are the values specified in BIP32 for keys on the main bitcoin network.

```
CK_ATTRIBUTE pubTemplate[] =
{
    {CKA_TOKEN,          &bToken,      sizeof(bToken)},
    {CKA_PRIVATE,       &bTrue,       sizeof(bTrue)},
    {CKA_ENCRYPT,       &bTrue,       sizeof(bTrue)},
    {CKA_VERIFY,       &bTrue,       sizeof(bTrue)},
    {CKA_MODIFIABLE,   &bTrue,       sizeof(bTrue)},
    {CKA_LABEL,        pbLabel,      strlen(pbLabel)},
};
CK_ATTRIBUTE privTemplate[] =
{
    {CKA_TOKEN,          &bToken,      sizeof(bToken)},
    {CKA_PRIVATE,       &bTrue,       sizeof(bTrue)},
    {CKA_SENSITIVE,    &bTrue,       sizeof(bTrue)},
    {CKA_SIGN,         &bTrue,       sizeof(bTrue)},
    {CKA_DECRYPT,       &bTrue,       sizeof(bTrue)},
    {CKA_MODIFIABLE,   &bTrue,       sizeof(bTrue)},
    {CKA_LABEL,        pbLabel,      strlen(pbLabel)},
};

CK_ULONG path[] = {
    CKF_BIP32_HARDENED | CKG_BIP44_PURPOSE,
    CKF_BIP32_HARDENED | CKG_BIP44_COIN_TYPE_BTC,
    CKF_BIP32_HARDENED | 1,
    CKG_BIP32_EXTERNAL_CHAIN,
    0
};

CK_BIP32_MASTER_DERIVE_PARAMS mechParams;
mechParams.pPublicKeyTemplate = pubTemplate;
mechParams.ulPublicKeyAttributeCount = ARRAY_SIZE(pubTemplate);
mechParams.pPrivateKeyTemplate = privTemplate;
mechParams.ulPrivateKeyAttributeCount = ARRAY_SIZE(privTemplate);
mechParams.pulPath = path;
mechParams.ulPathLen = ARRAY_SIZE(path);
CK_MECHANISM mechanism = {CKM_BIP32_CHILD_DERIVE, &mechParams, sizeof(mechParams)};

CK_RV rv = C_DeriveKey(hSession, &mechanism, hMasterPrivKey, NULL, 0, NULL);
// fail if rv != CKR_OK

CK_OBJECT_HANDLE pubKey = mechanism.hPublicKey;
CK_OBJECT_HANDLE privKey = mechanism.hPrivateKey;
```

The new key handles are stored in `pubKey` and `privKey` if the derivation was successful. The path generates a key pair that follows the BIP44 convention and can be used to receive BTC.

Importing a public extended key

```
CK_ATTRIBUTE template[] =
{
    {CKA_TOKEN,          &bToken,      sizeof(bToken)},
```

```

    {CKA_PRIVATE,          &bTrue,          sizeof(bTrue)},
    {CKA_DERIVE,          &bTrue,          sizeof(bTrue)},
    {CKA_MODIFIABLE,     &bTrue,          sizeof(bTrue)},
    {CKA_LABEL,          pbLabel,          strlen(pbLabel)},
};

```

```

CK_CHAR_PTR encodedKey = "xpub661MyMwAqRbcFtXgS5..."; //BIP32 serialization format
CK_OBJECT_HANDLE pubKey;

```

```

CK_RV rv = CA_Bip32ImportKey(hSession, template, ARRAY_SIZE(template), encodedKey, &pubKey);

```

The handle for the newly create key is stored in `pubKey` if the import was successful.

Exporting a public extended key

```

CK_CHAR encodedKey[CKG_BIP32_MAX_SERIALIZED_LEN+1];
CK_ULONG ulEncodedKeySize = sizeof(encodedKey);

```

```

CK_RV rv = CA_Bip32ExportPubKey(hSession, hObject, encodedKey, &ulEncodedKeySize );

```

The encoded key is stored in `encodedKey` (BIP32 serialization format) if there were no errors.

Importing a private extended key

```

CK_ATTRIBUTE template[] =
{
    {CKA_CLASS          &keyClass,    sizeof(keyClass)},
    {CKA_TOKEN,         &bToken,      sizeof(bToken)},
    {CKA_KEY_TYPE       &keyType,     sizeof(keyType)},
    {CKA_PRIVATE,       &bTrue,       sizeof(bTrue)},
    {CKA_DERIVE,        &bTrue,       sizeof(bTrue)},
    {CKA_MODIFIABLE,    &bTrue,       sizeof(bTrue)},
    {CKA_LABEL,         pbLabel,      strlen(pbLabel)},
    {CKA_SENSITIVE      &bTrue,       sizeof(bTrue)},
};

```

```

CK_CHAR_PTR encodedKey = "xprv9s21ZrQH143K3QTDL4LXw2F...";
CK_MECHANISM mechanism = {CKM_AES_KWP, NULL, 0};
CK_BYTE wrappedKey[256];
CK_ULONG wrappedKeyLen = sizeof(wrappedKey);
CK_OBJECT_HANDLE hUnwrappedKey;

```

```

CK_RV rv = C_EncryptInit(hSession, &mechanism, hWrappingKey);
// fail if rv != CKR_OK

```

```

rv = C_Encrypt(hSession, encodedKey, sizeof(encodedKey), wrappedKey, &wrappedKeyLen);
// fail if rv != CKR_OK

```

```

rv = C_UnwrapKey(hSession, &mechanism, hWrappingKey, wrappedKey, wrappedKeyLen, template, ARRAY_
SIZE(template), &hUnwrappedKey);

```

After unwrapping, the encoded key's BIP32 serialization format is decoded (the template key type is checked for BIP32). The handle of the unwrapped key is stored in `hUnwrappedKey` if there were no errors.

Exporting a private extended key

```

CK_MECHANISM mechanism = {CKM_AES_KWP, NULL, 0};
CK_BYTE key[256];
CK_ULONG keyLen = sizeof(key);

```

```

CK_RV rv = C_WrapKey(hSession, &mechanism, hWrappingKey, hKeyToWrap, key, &keyLen);

```

```
// fail if rv != CKR_OK

rv = C_DecryptInit(hSession, &mechanism, hWrappingKey);
// fail if rv != CKR_OK

rv = C_Decrypt(hSession, key, keyLen, key, &keyLen);
// fail if rv != CKR_OK

key[keyLen] = 0 // The key isn't NULL terminated after C_Decrypt().
C_WrapKey() must convert the BIP32 key to the BIP32 serialization format before wrapping.

The serialized key is stored in key if there were no errors.
```

PKCS#11 Definitions

```
#define CKK_BIP32 (CKK_VENDOR_DEFINED | 0x14)
#define CKM_BIP32_MASTER_DERIVE (CKM_VENDOR_DEFINED | 0xE00)
#define CKM_BIP32_CHILD_DERIVE (CKM_VENDOR_DEFINED | 0xE01)
#define CKR_BIP32_CHILD_INDEX_INVALID (CKR_VENDOR_DEFINED | 0x83)
#define CKR_BIP32_INVALID_HARDENED_DERIVATION (CKR_VENDOR_DEFINED | 0x84)
#define CKR_BIP32_MASTER_SEED_LEN_INVALID (CKR_VENDOR_DEFINED | 0x85)
#define CKR_BIP32_MASTER_SEED_INVALID (CKR_VENDOR_DEFINED | 0x86)
#define CKR_BIP32_INVALID_KEY_PATH_LEN (CKR_VENDOR_DEFINED | 0x87)
#define CKA_BIP32_CHAIN_CODE (CKA_VENDOR_DEFINED | 0x1100)
#define CKA_BIP32_VERSION_BYTES (CKA_VENDOR_DEFINED | 0x1101)
#define CKA_BIP32_CHILD_INDEX (CKA_VENDOR_DEFINED | 0x1102)
#define CKA_BIP32_CHILD_DEPTH (CKA_VENDOR_DEFINED | 0x1103)
#define CKA_BIP32_ID (CKA_VENDOR_DEFINED | 0x1104)
#define CKA_BIP32_FINGERPRINT (CKA_VENDOR_DEFINED | 0x1105)
#define CKA_BIP32_PARENT_FINGERPRINT (CKA_VENDOR_DEFINED | 0x1106)
#define CKG_BIP32_VERSION_MAINNET_PUB (0x0488B21E)
#define CKG_BIP32_VERSION_MAINNET_PRIV (0x0488ADE4)
#define CKG_BIP32_VERSION_TESTNET_PUB (0x043587CF)
#define CKG_BIP32_VERSION_TESTNET_PRIV (0x04358394)
#define CKG_BIP44_PURPOSE (0x0000002C)
#define CKG_BIP44_COIN_TYPE_BTC (0x00000000)
#define CKG_BIP44_COIN_TYPE_BTC_TESTNET (0x00000001)
#define CKG_BIP32_EXTERNAL_CHAIN (0x00000000)
#define CKG_BIP32_INTERNAL_CHAIN (0x00000001)
#define CKG_BIP32_MAX_SERIALIZED_LEN (112)
#define CKF_BIP32_HARDENED (0x80000000)
#define CKF_BIP32_MAX_PATH_LEN (255)
```

Derive Template

The `CKA_DERIVE_TEMPLATE` attribute is an optional extension to the `C_DeriveKey` function. This attribute points to an array template which provides additional security by restricting important attributes in the resulting derived key. This derive template, along with the user-supplied application template (called `pTemplate` in the PKCS#11 specification), determine the attributes of the derived key.

To invoke a derive template, the base key must have the `CKA_DERIVE_TEMPLATE` attribute set, pointing to a user-supplied derive template. When you specify this attribute on the base key and then attempt to derive a key, the derive operation adds the attributes of the application template to the attributes in the derive template. If there are any mismatches between attribute values specified in the two templates, the derive operation fails. Otherwise, the operation succeeds, producing a derived key with the combined attributes of the two templates.

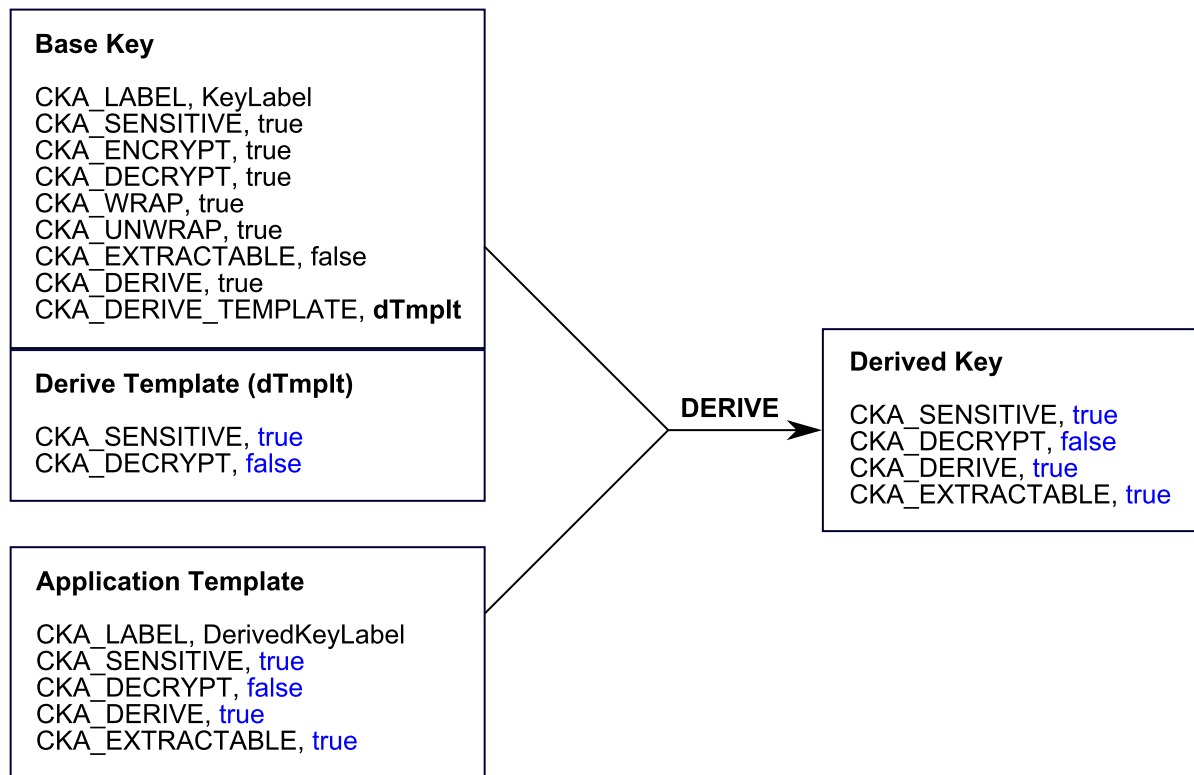
Any and all attributes which are valid for application template of a particular mechanism are also valid for the derive template. For security, the most effective attributes to restrict are those which might allow the derived key to be misused or expose secret information. Broadly these include but are not limited to encryption/decryption capabilities, extractability, the CKA_SENSITIVE attribute and the CKA_MODIFIABLE attribute. All mechanisms which support key derivation also support derive templates.

Examples

The following examples show a successful derivation with a derive template, and a failed derivation.

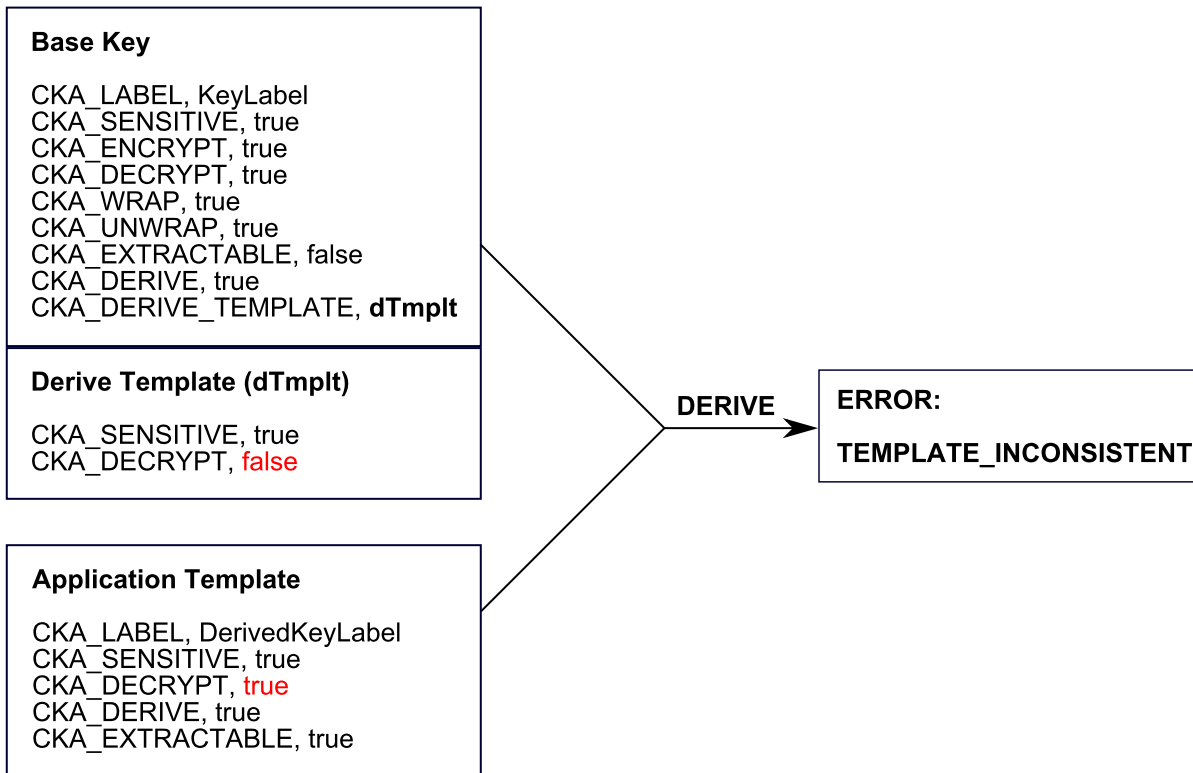
Successful Derivation

Here, the base key has the CKA_DERIVE_TEMPLATE attribute pointing to the derive template dTmplt. There are no conflicts between dTmplt and the application template. The application template's extra attributes are added to dTmplt's attributes, and the derivation operation produces a derived key containing the attributes in the two templates.



Failed Derivation

Here, the base key has the CKA_DERIVE_TEMPLATE attribute pointing to the derive template dTmplt. Notice that dTmplt has the CKA_DECRYPT attribute set to false, where the application template has the CKA_DECRYPT attribute set to true. This conflict causes the derivation operation to fail with the error TEMPLATE_INCONSISTENT.



CHAPTER 4: Supported Mechanisms

This chapter provides an alphabetical listing of the supported PKCS#11 standard mechanisms and Thales Group-proprietary mechanisms supported in firmware 7.4.0.

CKM_AES_CBC

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	AES
Algorithms	AES
Modes	CBC
Flags	Extractable

CKM_AES_CBC_ENCRYPT_DATA

Summary

FIPS approved?	Yes
Supported functions	Derive
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	0
Digest size	0
Key types	AES
Algorithms	None
Modes	None
Flags	None

CKM_AES_CBC_PAD

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	AES
Algorithms	AES
Modes	CBC_PAD
Flags	Extractable

CKM_AES_CBC_PAD_IPSEC

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	AES
Algorithms	AES
Modes	CBC_PAD_IPSEC
Flags	Extractable

CKM_AES_CFB8

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	16
Digest size	1
Key types	AES
Algorithms	AES
Modes	CFB
Flags	Extractable

CKM_AES_CFB128

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	16
Digest size	16
Key types	AES
Algorithms	AES
Modes	CFB
Flags	Extractable

CKM_AES_CMACH

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	AES
Algorithms	AES
Modes	MAC
Flags	Extractable CMACH

CKM_AES_CMACH_GENERAL

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	AES
Algorithms	AES
Modes	MAC
Flags	Extractable CMAC

CKM_AES_CTR

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	AES
Algorithms	AES
Modes	CTR
Flags	Extractable

CKM_AES_ECB

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	AES
Algorithms	AES
Modes	ECB
Flags	Extractable

CKM_AES_ECB_ENCRYPT_DATA

Summary

FIPS approved?	Yes
Supported functions	Derive
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	0
Digest size	0
Key types	AES
Algorithms	None
Modes	None
Flags	None

CKM_AES_GCM

GCM is the Galois/Counter Mode of operation of the AES algorithm for symmetric key encryption.

Usage Notes

Data size

The maximum allowed data size for this mechanism is 64KB (64 * 1024).

Initialization Vector (IV)

Random initialization vector (IV) is supported and recommended for GCM and for GMAC. In FIPS mode, the HSM firmware does not accept the IV parameter, and instead returns a generated IV.

The internal IV is a randomly generated 16-byte IV.

JCPROV

AES-GMAC and AES-GCM are supported in JCPROV. Use CK_AES_CMCMAC_PARAMS.java to define the GMAC operation. Implementation is the same as for PKCS#11.

Accumulating data

Our GMAC and GCM are single part operations, so even if they are called using multi-part API, we accumulate the data (up to a maximum) and return data only on the “final” operation. That is the meaning of “Accumulating” in the table, below.

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	AES
Algorithms	AES

Modes	GCM
Flags	Extractable Accumulating

CKM_AES_GMAC

GCM is the Galois/Counter Mode of operation of the AES algorithm for symmetric key encryption.

GMAC is a variant of GCM for sign/verify operation. If GCM input is confined to data that will not be encrypted, then GMAC is purely an authentication mode on the input data. The SafeNet Luna PCIe HSM GMAC implementation, formerly invoked only via PKCS#11 interface, can now be accessed via JC PROV and via our Java Provider (see Notes, below).

The GMAC implementation follows NIST SP-800-38D. It supports AES symmetric key sizes of 128, 192, and 256 bits.

Usage Notes

Initialization Vector (IV)

If the HSM is in FIPS mode (see HSM policy 12 at [HSM Capabilities and Policies](#)), the initialization vector (IV) is generated in the HSM and returned to the PKCS#11 function call. The buffer must be large enough to store the GMAC tag plus the generated IV (which has a length of 16 bytes).

If the HSM is **not** in FIPS mode, then the developer is responsible to specify an IV. Random IV is supported and recommended for GCM and GMAC. If you are not using random IV, then the most efficient IV value length is 12 bytes; any other size reduces performance and requires more work (per NIST SP-800-38D).

The internal IV is a randomly generated 16-byte IV.

Performance

For authentication, it is possible to use CKM_AES_GCM mechanism, when passing no data to encrypt (for strict compliance with NIST specification), and performance in that mode is better than in previous SafeNet releases.

The correlation is not exact but, as a general rule for a given mechanism, invocation by PKCS#11 API always provides the best performance, JSP performance is close but lower due to Java architecture, and JC PROV performance is somewhat lower still than PKCS#11 and JSP performance levels.

JC PROV

AES-GMAC and AES-GCM are supported in JC PROV. Use CK_AES_CMACH_PARAMS.java to define the GMAC operation. Implementation is the same as for PKCS#11.

Java Provider (JSP)

Both GMC and GMAC are supported. "GmacAesDemo.java" provides a sample for using GMAC with Java.

Java Parameter Specification class LunaGmacParameterSpec.java defines default values recommended by the NIST specification.

Accumulating Data

Our GMAC and GCM are single part operations, so even if they are called using multi-part API, we accumulate the data (up to a maximum) and return data only on the "final" operation. That is the meaning of "Accumulating" in the table, below.

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	AES
Algorithms	AES
Modes	GCM
Flags	Extractable Accumulating

CKM_AES_KEY_GEN

Summary

FIPS approved?	Yes
Supported functions	Generate Key
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	0
Digest size	0
Key types	AES
Algorithms	None
Modes	None
Flags	None

CKM_AES_KW

NIST Special Publication 800-38F describes cryptographic methods that are approved for “key wrapping,” that is, the protection of the confidentiality and integrity of cryptographic keys. In addition to describing existing methods, that publication specifies two new, deterministic authenticated-encryption modes of operation of the Advanced Encryption Standard (AES) algorithm: the AES Key Wrap (KW) mode and the AES Key Wrap With Padding (KWP) mode. Gemalto's SafeNet Luna PCIe HSM implements the AES Key Wrap (KW) mode at this time, which SP800-38F recommends as more secure than CKM_AES_CBC.

NOTE NIST Special Publication 800-38F recommends this method as more secure than CKM_AES_CBC.

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	8
Digest size	0
Key types	AES
Algorithms	AES
Modes	KEYWRAP
Flags	Extractable Accumulating

CKM_AES_KWP

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	8
Digest size	0
Key types	AES
Algorithms	AES
Modes	KEYWRAP_PAD
Flags	Extractable Accumulating

CKM_AES_MAC

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	AES
Algorithms	AES
Modes	MAC
Flags	Extractable

CKM_AES_MAC_GENERAL

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	AES
Algorithms	AES
Modes	MAC
Flags	Extractable

CKM_AES_OFB

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	AES
Algorithms	AES
Modes	OFB
Flags	Extractable

CKM_AES_XTS

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	AES
Algorithms	AES
Modes	XTS
Flags	Extractable

CKM_ARIA_CBC

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	ARIA
Algorithms	ARIA
Modes	CBC
Flags	Extractable

CKM_ARIA_CBC_ENCRYPT_DATA

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	0
Digest size	0
Key types	ARIA
Algorithms	None
Modes	None
Flags	None

CKM_ARIA_CBC_PAD

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	ARIA
Algorithms	ARIA
Modes	CBC_PAD
Flags	Extractable

CKM_ARIA_CFB8

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	1
Key types	ARIA
Algorithms	ARIA
Modes	CFB
Flags	Extractable

CKM_ARIA_CFB128

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	16
Key types	ARIA
Algorithms	ARIA
Modes	CFB
Flags	Extractable

CKM_ARIA_CMACH

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	ARIA
Algorithms	ARIA
Modes	MAC
Flags	Extractable CMACH

CKM_ARIA_CMACH_GENERAL

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	ARIA
Algorithms	ARIA
Modes	MAC
Flags	Extractable CMAC

CKM_ARIA_CTR

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	ARIA
Algorithms	ARIA
Modes	CTR
Flags	Extractable

CKM_ARIA_ECB

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	ARIA
Algorithms	ARIA
Modes	ECB
Flags	Extractable

CKM_ARIA_ECB_ENCRYPT_DATA

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	0
Digest size	0
Key types	ARIA
Algorithms	None
Modes	None
Flags	None

CKM_ARIA_KEY_GEN

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	0
Digest size	0
Key types	ARIA
Algorithms	None
Modes	None
Flags	None

CKM_ARIA_L_CBC

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Decrypt Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	ARIA
Algorithms	ARIA
Modes	CBC
Flags	Extractable

CKM_ARIA_L_CBC_PAD

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Decrypt Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	ARIA
Algorithms	ARIA
Modes	CBC_PAD
Flags	Extractable

CKM_ARIA_L_ECB

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Decrypt Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	ARIA
Algorithms	ARIA
Modes	ECB
Flags	Extractable

CKM_ARIA_L_MAC

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	ARIA
Algorithms	ARIA
Modes	MAC
Flags	Extractable

CKM_ARIA_L_MAC_GENERAL

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	ARIA
Algorithms	ARIA
Modes	MAC
Flags	Extractable

CKM_ARIA_MAC

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	ARIA
Algorithms	ARIA
Modes	MAC
Flags	Extractable

CKM_ARIA_MAC_GENERAL

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	ARIA
Algorithms	ARIA
Modes	MAC
Flags	Extractable

CKM_ARIA_OFB

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	16
Digest size	0
Key types	ARIA
Algorithms	ARIA
Modes	OFB
Flags	Extractable

CKM_BIP32_CHILD_DERIVE

This mechanism is used to derive child keys from a parent key, and can generate both the private and public part of the key pair, accepting a BIP32 public or private key as input.

Cloning (or backup) of BIP32 keys can be performed only between PCIe and/or Network HSMs containing firmware versions that support BIP32.

See "[BIP32 Mechanism Support and Implementation](#)" on page 48.

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	0
Digest size	0
Key types	BIP32
Algorithms	None
Modes	None
Flags	Extractable

CKM_BIP32_MASTER_DERIVE

This mechanism is used to derive the master key pair from a seed. The input key must have the type `CKK_GENERIC_SECRET` (size between 128 and 512 bits).

Only curve `secp256k1` is supported. Key type `CKK_BIP32` is introduced; existing ECDSA keys cannot be used with the BIP32 mechanisms. All mechanisms supported by ECDSA keys are supported for BIP32 keys.

Cloning (or backup) of BIP32 keys can be performed only between PCIe and/or Network HSMs containing firmware versions that support BIP32.

See ["BIP32 Mechanism Support and Implementation" on page 48](#).

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	512
Block size	0
Digest size	0
Key types	GENERIC_SECRET
Algorithms	None
Modes	None
Flags	Extractable

CKM_CAST3_CBC

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	8
Digest size	0
Key types	CAST3
Algorithms	CAST3
Modes	CBC
Flags	Extractable

CKM_CAST3_CBC_PAD

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	8
Digest size	0
Key types	CAST3
Algorithms	CAST3
Modes	CBC_PAD
Flags	Extractable

CKM_CAST3_ECB

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	8
Digest size	0
Key types	CAST3
Algorithms	CAST3
Modes	ECB
Flags	Extractable

CKM_CAST3_KEY_GEN

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	0
Digest size	0
Key types	CAST3
Algorithms	None
Modes	None
Flags	None

CKM_CAST3_MAC

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	8
Digest size	0
Key types	CAST3
Algorithms	CAST3
Modes	MAC
Flags	Extractable

CKM_CAST3_MAC_GENERAL

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	8
Digest size	0
Key types	CAST3
Algorithms	CAST3
Modes	MAC
Flags	Extractable

CKM_CAST5_CBC

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	8
Digest size	0
Key types	CAST5
Algorithms	CAST5
Modes	CBC
Flags	Extractable

CKM_CAST5_CBC_PAD

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	8
Digest size	0
Key types	CAST5
Algorithms	CAST5
Modes	CBC_PAD
Flags	Extractable

CKM_CAST5_ECB

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	8
Digest size	0
Key types	CAST5
Algorithms	CAST5
Modes	ECB
Flags	Extractable

CKM_CAST5_KEY_GEN

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	0
Digest size	0
Key types	CAST5
Algorithms	None
Modes	None
Flags	None

CKM_CAST5_MAC

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	8
Digest size	0
Key types	CAST5
Algorithms	CAST5
Modes	MAC
Flags	Extractable

CKM_CAST5_MAC_GENERAL

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	8
Digest size	0
Key types	CAST5
Algorithms	CAST5
Modes	MAC
Flags	Extractable

CKM_DES_CBC

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	8
Digest size	0
Key types	DES
Algorithms	DES
Modes	CBC
Flags	Extractable

CKM_DES_CBC_ENCRYPT_DATA

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	0
Digest size	0
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

CKM_DES_CBC_PAD

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	8
Digest size	0
Key types	DES
Algorithms	DES
Modes	CBC_PAD
Flags	Extractable

CKM_DES_CFB8

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	192
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	192
Block size	8
Digest size	1
Key types	DES3
Algorithms	DES3
Modes	CFB
Flags	Extractable

CKM_DES_CFB64

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	192
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	192
Block size	8
Digest size	8
Key types	DES3
Algorithms	DES3
Modes	CFB
Flags	Extractable

CKM_DES_ECB

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	8
Digest size	0
Key types	DES
Algorithms	DES
Modes	ECB
Flags	Extractable

CKM_DES_ECB_ENCRYPT_DATA

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	0
Digest size	0
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

CKM_DES_KEY_GEN

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	0
Digest size	0
Key types	DES
Algorithms	None
Modes	None
Flags	None

CKM_DES_MAC

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	8
Digest size	0
Key types	DES
Algorithms	DES
Modes	MAC
Flags	Extractable

CKM_DES_MAC_GENERAL

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	8
Digest size	0
Key types	DES
Algorithms	DES
Modes	MAC
Flags	Extractable

CKM_DES_OFB64

Summary

CKM_DES2_DUKPT_DATA

The CKM_DES2_DUKPT family of key derive mechanisms create keys used to protect EFTPOS terminal sessions. The mechanisms implement the algorithm for server side DUKPT derivation as defined by ANSI X9.24 part 1.

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	192
Block size	0
Digest size	0
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

Usage

This mechanism has the following attributes:

- > Only CKK_DES2 keys can be derived. The mechanism will force the CKA_KEY_TYPE attribute of the derived object to equal CKK_DES2. If the template does specify a CKA_KEY_TYPE attribute then it must be CKK_DES2.
- > The mechanism takes a CK_KEY_DERIVATION_STRING_DATA structure as a parameter.
- > The pData field of the parameter must point to a 10 byte array which holds the 80 bit Key Sequence Number (KSN).
- > This mechanism contributes the CKA_CLASS and CKA_KEY_TYPE and CKA_VALUE to the resulting object.

The DUKPT MAC and DATA versions will default to the appropriate usage mechanism as described in the following table:

Mechanism	CKA_SIGN	CKA_VERIFY	CKA_DECRYPT	CKA_ENCRYPT
CKM_DES2_DUKPT_MAC	True	True		
CKM_DES2_DUKPT_MAC_RESP	True			
CKM_DES2_DUKPT_DATA			True	True
CKM_DES2_DUKPT_DATA_RESP				True

Example

```
#define CKM_DES2_DUKPT_PIN                (CKM_VENDOR_DEFINED + 0x611)
#define CKM_DES2_DUKPT_MAC                (CKM_VENDOR_DEFINED + 0x612)
#define CKM_DES2_DUKPT_MAC_RESP          (CKM_VENDOR_DEFINED + 0x613)
#define CKM_DES2_DUKPT_DATA              (CKM_VENDOR_DEFINED + 0x614)
#define CKM_DES2_DUKPT_DATA_RESP         (CKM_VENDOR_DEFINED + 0x615)

CK_OBJECT_HANDLE hBDKey; // handle of CKK_DES2 or CKK_DES2 Base Derive Key
CK_OBJECT_HANDLE hMKey;  // handle of CKK_DES2 MAC session Key
CK_MECHANISM svMech = { CKM_DES3_X919_MAC , NULL, 0};

CK_KEY_DERIVATION_STRING_DATA param;
CK_MECHANISM kdMech = { CKM_DES2_DUKPT_MAC , NULL, 0};
CK_CHAR ksn[10];
CK_CHAR inp[any length];
CK_CHAR mac[4];
CK_SIZE len;

// Derive MAC verify session key
param.pData=ksn;
param.ulLen = 10;

kdMech.mechanism = CKM_DES2_DUKPT_MAC;
kdMech.pParameter = &param;
kdMech.ulParameterLen = sizeof parram;

C_DeriveKey(hSes, &kdMech, hBDKey , NULL, 0, &hMKey);

// Single part verify operation

C_VerifyInit(hSes, &svMech, hMKey);
len = sizeof mac;
C_Verify(hSes, inp, sizeof inp, mac, len);

// clean up

C_DestroyObject(hSes, hMKey);

// Test vectors
```

CKM_DES2_DUKPT_DATA_RESP

The CKM_DES2_DUKPT family of key derive mechanisms create keys used to protect EFTPOS terminal sessions. The mechanisms implement the algorithm for server side DUKPT derivation as defined by ANSI X9.24 part 1.

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	192
Block size	0
Digest size	0
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

Usage

This mechanism has the following attributes:

- > Only CKK_DES2 keys can be derived. The mechanism will force the CKA_KEY_TYPE attribute of the derived object to equal CKK_DES2. If the template does specify a CKA_KEY_TYPE attribute then it must be CKK_DES2.
- > The mechanism takes a CK_KEY_DERIVATION_STRING_DATA structure as a parameter.
- > The pData field of the parameter must point to a 10 byte array which holds the 80 bit Key Sequence Number (KSN).
- > This mechanism contributes the CKA_CLASS and CKA_KEY_TYPE and CKA_VALUE to the resulting object.

The DUKPT MAC and DATA versions will default to the appropriate usage mechanism as described in the following table:

Mechanism	CKA_SIGN	CKA_VERIFY	CKA_DECRYPT	CKA_ENCRYPT
CKM_DES2_DUKPT_MAC	True	True		
CKM_DES2_DUKPT_MAC_RESP	True			
CKM_DES2_DUKPT_DATA			True	True
CKM_DES2_DUKPT_DATA_RESP				True

Example

```
#define CKM_DES2_DUKPT_PIN                (CKM_VENDOR_DEFINED + 0x611)
#define CKM_DES2_DUKPT_MAC                (CKM_VENDOR_DEFINED + 0x612)
#define CKM_DES2_DUKPT_MAC_RESP          (CKM_VENDOR_DEFINED + 0x613)
#define CKM_DES2_DUKPT_DATA              (CKM_VENDOR_DEFINED + 0x614)
#define CKM_DES2_DUKPT_DATA_RESP        (CKM_VENDOR_DEFINED + 0x615)

CK_OBJECT_HANDLE hBDKey; // handle of CKK_DES2 or CKK_DES2 Base Derive Key
CK_OBJECT_HANDLE hMKey;  // handle of CKK_DES2 MAC session Key
CK_MECHANISM svMech = { CKM_DES3_X919_MAC , NULL, 0};

CK_KEY_DERIVATION_STRING_DATA param;
CK_MECHANISM kdMech = { CKM_DES2_DUKPT_MAC , NULL, 0};
CK_CHAR ksn[10];
CK_CHAR inp[any length];
CK_CHAR mac[4];
CK_SIZE len;

// Derive MAC verify session key
param.pData=ksn;
param.ulLen = 10;

kdMech.mechanism = CKM_DES2_DUKPT_MAC;
kdMech.pParameter = &param;
kdMech.ulParameterLen = sizeof parram;

C_DeriveKey(hSes, &kdMech, hBDKey , NULL, 0, &hMKey);

// Single part verify operation

C_VerifyInit(hSes, &svMech, hMKey);
len = sizeof mac;
C_Verify(hSes, inp, sizeof inp, mac, len);

// clean up

C_DestroyObject(hSes, hMKey);

// Test vectors
```

CKM_DES2_DUKPT_MAC

The CKM_DES2_DUKPT family of key derive mechanisms create keys used to protect EFTPOS terminal sessions. The mechanisms implement the algorithm for server side DUKPT derivation as defined by ANSI X9.24 part 1.

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	192
Block size	0
Digest size	0
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

Usage

This mechanism has the following attributes:

- > Only CKK_DES2 keys can be derived. The mechanism will force the CKA_KEY_TYPE attribute of the derived object to equal CKK_DES2. If the template does specify a CKA_KEY_TYPE attribute then it must be CKK_DES2.
- > The mechanism takes a CK_KEY_DERIVATION_STRING_DATA structure as a parameter.
- > The pData field of the parameter must point to a 10 byte array which holds the 80 bit Key Sequence Number (KSN).
- > This mechanism contributes the CKA_CLASS and CKA_KEY_TYPE and CKA_VALUE to the resulting object.

The DUKPT MAC and DATA versions will default to the appropriate usage mechanism as described in the following table:

Mechanism	CKA_SIGN	CKA_VERIFY	CKA_DECRYPT	CKA_ENCRYPT
CKM_DES2_DUKPT_MAC	True	True		
CKM_DES2_DUKPT_MAC_RESP	True			
CKM_DES2_DUKPT_DATA			True	True
CKM_DES2_DUKPT_DATA_RESP				True

Example

```
#define CKM_DES2_DUKPT_PIN                (CKM_VENDOR_DEFINED + 0x611)
#define CKM_DES2_DUKPT_MAC                (CKM_VENDOR_DEFINED + 0x612)
#define CKM_DES2_DUKPT_MAC_RESP           (CKM_VENDOR_DEFINED + 0x613)
#define CKM_DES2_DUKPT_DATA               (CKM_VENDOR_DEFINED + 0x614)
#define CKM_DES2_DUKPT_DATA_RESP          (CKM_VENDOR_DEFINED + 0x615)

CK_OBJECT_HANDLE hBDKey; // handle of CKK_DES2 or CKK_DES2 Base Derive Key
CK_OBJECT_HANDLE hMKey;  // handle of CKK_DES2 MAC session Key
CK_MECHANISM svMech = { CKM_DES2_X919_MAC , NULL, 0};

CK_KEY_DERIVATION_STRING_DATA param;
CK_MECHANISM kdMech = { CKM_DES2_DUKPT_MAC , NULL, 0};
CK_CHAR ksn[10];
CK_CHAR inp[any length];
CK_CHAR mac[4];
CK_SIZE len;

// Derive MAC verify session key
param.pData=ksn;
param.ulLen = 10;

kdMech.mechanism = CKM_DES2_DUKPT_MAC;
kdMech.pParameter = &param;
kdMech.ulParameterLen = sizeof parram;

C_DeriveKey(hSes, &kdMech, hBDKey , NULL, 0, &hMKey);

// Single part verify operation

C_VerifyInit(hSes, &svMech, hMKey);
len = sizeof mac;
C_Verify(hSes, inp, sizeof inp, mac, len);

// clean up

C_DestroyObject(hSes, hMKey);

// Test vectors
```

CKM_DES2_DUKPT_MAC_RESP

The CKM_DES2_DUKPT family of key derive mechanisms create keys used to protect EFTPOS terminal sessions. The mechanisms implement the algorithm for server side DUKPT derivation as defined by ANSI X9.24 part 1.

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	192
Block size	0
Digest size	0
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

Usage

This mechanism has the following attributes:

- > Only CKK_DES2 keys can be derived. The mechanism will force the CKA_KEY_TYPE attribute of the derived object to equal CKK_DES2. If the template does specify a CKA_KEY_TYPE attribute then it must be CKK_DES2.
- > The mechanism takes a CK_KEY_DERIVATION_STRING_DATA structure as a parameter.
- > The pData field of the parameter must point to a 10 byte array which holds the 80 bit Key Sequence Number (KSN).
- > This mechanism contributes the CKA_CLASS and CKA_KEY_TYPE and CKA_VALUE to the resulting object.

The DUKPT MAC and DATA versions will default to the appropriate usage mechanism as described in the following table:

Mechanism	CKA_SIGN	CKA_VERIFY	CKA_DECRYPT	CKA_ENCRYPT
CKM_DES2_DUKPT_MAC	True	True		
CKM_DES2_DUKPT_MAC_RESP	True			
CKM_DES2_DUKPT_DATA			True	True
CKM_DES2_DUKPT_DATA_RESP				True

Example

```

#define CKM_DES2_DUKPT_PIN                (CKM_VENDOR_DEFINED + 0x611)
#define CKM_DES2_DUKPT_MAC                (CKM_VENDOR_DEFINED + 0x612)
#define CKM_DES2_DUKPT_MAC_RESP          (CKM_VENDOR_DEFINED + 0x613)
#define CKM_DES2_DUKPT_DATA              (CKM_VENDOR_DEFINED + 0x614)
#define CKM_DES2_DUKPT_DATA_RESP        (CKM_VENDOR_DEFINED + 0x615)

CK_OBJECT_HANDLE hBDKey; // handle of CKK_DES2 or CKK_DES2 Base Derive Key
CK_OBJECT_HANDLE hMKey;  // handle of CKK_DES2 MAC session Key
CK_MECHANISM svMech = { CKM_DES3_X919_MAC , NULL, 0};

CK_KEY_DERIVATION_STRING_DATA param;
CK_MECHANISM kdMech = { CKM_DES2_DUKPT_MAC , NULL, 0};
CK_CHAR ksn[10];
CK_CHAR inp[any length];
CK_CHAR mac[4];
CK_SIZE len;

// Derive MAC verify session key
param.pData=ksn;
param.ulLen = 10;

kdMech.mechanism = CKM_DES2_DUKPT_MAC;
kdMech.pParameter = &param;
kdMech.ulParameterLen = sizeof parram;

C_DeriveKey(hSes, &kdMech, hBDKey , NULL, 0, &hMKey);

// Single part verify operation

C_VerifyInit(hSes, &svMech, hMKey);
len = sizeof mac;
C_Verify(hSes, inp, sizeof inp, mac, len);

// clean up

C_DestroyObject(hSes, hMKey);

// Test vectors

```

CKM_DES2_DUKPT_PIN

The CKM_DES2_DUKPT family of key derive mechanisms create keys used to protect EFTPOS terminal sessions. The mechanisms implement the algorithm for server side DUKPT derivation as defined by ANSI X9.24 part 1.

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	192
Block size	0
Digest size	0
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

Usage

This mechanism has the following attributes:

- > Only CKK_DES2 keys can be derived. The mechanism will force the CKA_KEY_TYPE attribute of the derived object to equal CKK_DES2. If the template does specify a CKA_KEY_TYPE attribute then it must be CKK_DES2.
- > The mechanism takes a CK_KEY_DERIVATION_STRING_DATA structure as a parameter.
- > The pData field of the parameter must point to a 10 byte array which holds the 80 bit Key Sequence Number (KSN).
- > This mechanism contributes the CKA_CLASS and CKA_KEY_TYPE and CKA_VALUE to the resulting object.

The DUKPT MAC and DATA versions will default to the appropriate usage mechanism as described in the following table:

Mechanism	CKA_SIGN	CKA_VERIFY	CKA_DECRYPT	CKA_ENCRYPT
CKM_DES2_DUKPT_MAC	True	True		
CKM_DES2_DUKPT_MAC_RESP	True			
CKM_DES2_DUKPT_DATA			True	True
CKM_DES2_DUKPT_DATA_RESP				True

Example

```
#define CKM_DES2_DUKPT_PIN                (CKM_VENDOR_DEFINED + 0x611)
#define CKM_DES2_DUKPT_MAC                (CKM_VENDOR_DEFINED + 0x612)
#define CKM_DES2_DUKPT_MAC_RESP           (CKM_VENDOR_DEFINED + 0x613)
#define CKM_DES2_DUKPT_DATA               (CKM_VENDOR_DEFINED + 0x614)
#define CKM_DES2_DUKPT_DATA_RESP          (CKM_VENDOR_DEFINED + 0x615)

CK_OBJECT_HANDLE hBDKey; // handle of CKK_DES2 or CKK_DES2 Base Derive Key
CK_OBJECT_HANDLE hMKey;  // handle of CKK_DES2 MAC session Key
CK_MECHANISM svMech = { CKM_DES3_X919_MAC , NULL, 0};

CK_KEY_DERIVATION_STRING_DATA param;
CK_MECHANISM kdMech = { CKM_DES2_DUKPT_MAC , NULL, 0};
CK_CHAR ksn[10];
CK_CHAR inp[any length];
CK_CHAR mac[4];
CK_SIZE len;

// Derive MAC verify session key
param.pData=ksn;
param.ulLen = 10;

kdMech.mechanism = CKM_DES2_DUKPT_MAC;
kdMech.pParameter = &param;
kdMech.ulParameterLen = sizeof parram;

C_DeriveKey(hSes, &kdMech, hBDKey , NULL, 0, &hMKey);

// Single part verify operation

C_VerifyInit(hSes, &svMech, hMKey);
len = sizeof mac;
C_Verify(hSes, inp, sizeof inp, mac, len);

// clean up

C_DestroyObject(hSes, hMKey);

// Test vectors
```

CKM_DES2_KEY_GEN

Summary

FIPS approved?	Yes
Supported functions	Generate Key
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	128
Block size	0
Digest size	0
Key types	DES2
Algorithms	None
Modes	None
Flags	None

CKM_DES3_CBC

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	192
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	192
Block size	8
Digest size	0
Key types	DES3
Algorithms	DES3
Modes	CBC
Flags	Extractable

CKM_DES3_CBC_ENCRYPT_DATA

Summary

FIPS approved?	Yes
Supported functions	Derive
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	192
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	192
Block size	0
Digest size	0
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

CKM_DES3_CBC_PAD

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	192
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	192
Block size	8
Digest size	0
Key types	DES3
Algorithms	DES3
Modes	CBC_PAD
Flags	Extractable

CKM_DES3_CBC_PAD_IPSEC

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	192
Block size	8
Digest size	0
Key types	DES3
Algorithms	DES3
Modes	CBC_PAD_IPSEC
Flags	Extractable

CKM_DES3_CMAC

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	192
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	192
Block size	8
Digest size	0
Key types	DES3
Algorithms	DES3
Modes	MAC
Flags	Extractable CMAC

CKM_DES3_CMAC_GENERAL

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	192
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	192
Block size	8
Digest size	0
Key types	DES3
Algorithms	DES3
Modes	MAC
Flags	Extractable CMAC

CKM_DES3_CTR

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	192
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	192
Block size	8
Digest size	0
Key types	DES3
Algorithms	DES3
Modes	CTR
Flags	Extractable

CKM_DES3_ECB

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	192
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	192
Block size	8
Digest size	0
Key types	DES3
Algorithms	DES3
Modes	ECB
Flags	Extractable

CKM_DES3_ECB_ENCRYPT_DATA

Summary

FIPS approved?	Yes
Supported functions	Derive
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	192
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	192
Block size	0
Digest size	0
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

CKM_DES3_KEY_GEN

Summary

FIPS approved?	Yes
Supported functions	Generate Key
Minimum key length (bits)	192
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	192
Maximum key length (bits)	192
Block size	0
Digest size	0
Key types	DES3
Algorithms	None
Modes	None
Flags	None

CKM_DES3_MAC

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	192
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	192
Block size	8
Digest size	0
Key types	DES3
Algorithms	DES3
Modes	MAC
Flags	Extractable

CKM_DES3_MAC_GENERAL

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	192
Minimum legacy key length for FIPS use (bits)	128
Maximum key length (bits)	192
Block size	8
Digest size	0
Key types	DES3
Algorithms	DES3
Modes	MAC
Flags	Extractable

CKM_DES3_X919_MAC

The CKM_DES3_X919_MAC is a signature generation and verification mechanism, as defined ANSI X9.19-1996 Financial Institution Retail Message Authentication annex 1 Cipher Block Chaining Procedure.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	192
Block size	8
Digest size	0
Key types	DES3
Algorithms	DES3
Modes	MAC
Flags	Extractable

Usage

The CKM_DES3_X919_MAC mechanism is used with the **C_VerifyInit** and **C_SignInit** functions. It has the following attributes:

- > Only CKK_DES2 and CKK_DES3 keys are supported.
- > The mechanism takes no parameter.
- > Multi-part operation is supported.
- > The total input data length must be at least one byte.
- > The length of result is half the size of the DES block (i.e. 4 bytes).

Example

```
#define CKM_DES3_X919_MAC (CKM_VENDOR_DEFINED + 0x150)

CK_OBJECT_HANDLE hKey; // handle of CKK_DES2 or CKK_DES3 key
CK_MECHANISM mech = { CKM_DES3_X919_MAC, NULL, 0};
```

```
CK_CHAR inp[any length];
CK_CHAR mac[4];
CK_SIZE len;

// Single-part operation

C_SignInit(hSes, &mech, hKey);
len = sizeof mac;
C_Sign(hSes, inp, sizeof inp, mac, &len);

// Multi-part operation

C_SignInit(hSes, &mech, hKey);
C_SignUpdate(hSes, inp, sizeof inp/2);
C_SignUpdate(hSes, inp+ (sizeof inp)/2, sizeof inp/2);
len = sizeof mac;
C_SignFinal(hSes, mac, &len);

// Test vectors

static const UInt8 retailKey[16] =
{
    0x58, 0x91, 0x25, 0x86, 0x3D, 0x46, 0x10, 0x7F,
    0x46, 0x3E, 0x52, 0x3B, 0xF7, 0x46, 0x9D, 0x52
};

static const UInt8 retailInputAscii[19] =
{
    't','h','e',' ','q','u','i','c','k',' ','b','r','o','w','n',' ','f','o','x'
};

static const UInt8 retailMACAscii[4] =
{
    0x55, 0xA7, 0xBF, 0xBA
};

static const UInt8 retailInputEBCDIC[19] =
{
    // "the quick brown fox" in EBCDIC
    0xA3, 0x88, 0x85, 0x40, 0x98, 0xA4, 0x89, 0x83,
    0x92, 0x40, 0x82, 0x99, 0x96, 0xA6, 0x95, 0x40,
    0x86, 0x96, 0xA7
};

static const UInt8 retailMACEBCDIC[4] =
{
    0x60, 0xAE, 0x2C, 0xD7
};
```

CKM_DH_PKCS_DERIVE

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	512
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	0
Digest size	0
Key types	DH
Algorithms	None
Modes	None
Flags	None

CKM_DH_PKCS_KEY_PAIR_GEN

Summary

FIPS approved?	No
Supported functions	Generate Key Pair
Minimum key length (bits)	512
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	0
Digest size	0
Key types	DH
Algorithms	None
Modes	None
Flags	None

CKM_DH_PKCS_PARAMETER_GEN

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	512
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	0
Digest size	0
Key types	DH
Algorithms	None
Modes	None
Flags	None

CKM_DSA

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	3072
Block size	0
Digest size	0
Key types	DSA
Algorithms	DSA
Modes	None
Flags	None

CKM_DSA_KEY_PAIR_GEN

Summary

FIPS approved?	Yes
Supported functions	Generate Key Pair
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	3072
Block size	0
Digest size	0
Key types	DSA
Algorithms	None
Modes	None
Flags	None

CKM_DSA_PARAMETER_GEN

Summary

FIPS approved?	Yes
Supported functions	Generate Key
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	3072
Block size	0
Digest size	0
Key types	DSA
Algorithms	None
Modes	None
Flags	None

CKM_DSA_SHA1

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	3072
Block size	64
Digest size	20
Key types	DSA
Algorithms	SHA
Modes	None
Flags	Extractable

CKM_DSA_SHA224

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	3072
Block size	64
Digest size	28
Key types	DSA
Algorithms	SHA224
Modes	None
Flags	Extractable

CKM_DSA_SHA256

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	3072
Block size	64
Digest size	32
Key types	DSA
Algorithms	SHA256
Modes	None
Flags	Extractable

CKM_EC_EDWARDS_KEY_PAIR_GEN

Summary

FIPS approved?	No
Supported functions	Generate Key Pair
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	0
Digest size	0
Key types	EDDSA
Algorithms	None
Modes	None
Flags	None

CKM_EC_KEY_PAIR_GEN

Summary

FIPS approved?	Yes
Supported functions	Generate Key Pair
Minimum key length (bits)	105
Minimum key length for FIPS use (bits)	224
Minimum legacy key length for FIPS use (bits)	160
Maximum key length (bits)	571
Block size	0
Digest size	0
Key types	ECDSA
Algorithms	None
Modes	None
Flags	None

CKM_EC_KEY_PAIR_GEN_W_EXTRA_BITS

Summary

FIPS approved?	Yes
Supported functions	Generate Key Pair
Minimum key length (bits)	105
Minimum key length for FIPS use (bits)	224
Minimum legacy key length for FIPS use (bits)	160
Maximum key length (bits)	571
Block size	0
Digest size	0
Key types	ECDSA
Algorithms	None
Modes	None
Flags	Extra bits

CKM_EC_MONTGOMERY_KEY_PAIR_GEN

Generate keys over Montgomery curves. Keys generated with this mechanism are of type CKK_EC_MONTGOMERY. They can be used with the existing CKM_ECDH1_DERIVE mechanism. Given that the ECDH mechanism is the same, and relies on "point multiply" on the given curve, no Montgomery-specific mechanism is provided at this time. Allowed curve is "Curve25519".

Summary

FIPS approved?	Yes
Supported functions	Generate Key Pair
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	256
Maximum key length (bits)	256
Block size	0
Digest size	0
Key types	EC_MONT
Algorithms	None
Modes	None
Flags	None

CKM_ECDH1_COFACTOR_DERIVE

Summary

FIPS approved?	Yes
Supported functions	Derive
Minimum key length (bits)	105
Minimum key length for FIPS use (bits)	224
Minimum legacy key length for FIPS use (bits)	160
Maximum key length (bits)	571
Block size	0
Digest size	0
Key types	ECDSA BIP32
Algorithms	None
Modes	None
Flags	None

CKM_ECDH1_DERIVE

Elliptic Curve Diffie-Hellman is an anonymous key-agreement protocol. CKM_ECDH1_DERIVE is the derive function for that protocol.

NOTE To enhance performance, we have created a proprietary call CA_DeriveKeyAndWrap, which is an optimization of C_DeriveKey with C_Wrap, merging the two functions into one (the in and out constraints are the same as for the individual functions). A further optimization is applied when mechanism CKM_ECDH1_DERIVE is used with CA_DeriveKeyAndWrap.

If CA_DeriveKeyAndWrap is called with other mechanisms, those would not be optimized.

Summary

FIPS approved?	Yes
Supported functions	Derive
Minimum key length (bits)	105
Minimum key length for FIPS use (bits)	224
Minimum legacy key length for FIPS use (bits)	160
Maximum key length (bits)	571
Block size	0
Digest size	0
Key types	ECDSA EC_MONT BIP32
Algorithms	None
Modes	None
Flags	None

CKM_ECDSA

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	105
Minimum key length for FIPS use (bits)	224
Minimum legacy key length for FIPS use (bits)	160
Maximum key length (bits)	571
Block size	0
Digest size	0
Key types	ECDSA BIP32
Algorithms	ECDSA
Modes	None
Flags	None

CKM_ECDSA_GBCS_SHA256

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	64
Digest size	32
Key types	ECDSA BIP32
Algorithms	SHA256
Modes	None
Flags	Extractable

CKM_ECDSA_SHA1

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	105
Minimum key length for FIPS use (bits)	224
Minimum legacy key length for FIPS use (bits)	160
Maximum key length (bits)	571
Block size	64
Digest size	20
Key types	ECDSA BIP32
Algorithms	SHA
Modes	None
Flags	Extractable

CKM_ECDSA_SHA224

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	105
Minimum key length for FIPS use (bits)	224
Minimum legacy key length for FIPS use (bits)	160
Maximum key length (bits)	571
Block size	64
Digest size	28
Key types	ECDSA BIP32
Algorithms	SHA224
Modes	None
Flags	Extractable

CKM_ECDSA_SHA256

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	105
Minimum key length for FIPS use (bits)	224
Minimum legacy key length for FIPS use (bits)	160
Maximum key length (bits)	571
Block size	64
Digest size	32
Key types	ECDSA BIP32
Algorithms	SHA256
Modes	None
Flags	Extractable

CKM_ECDSA_SHA384

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	105
Minimum key length for FIPS use (bits)	224
Minimum legacy key length for FIPS use (bits)	160
Maximum key length (bits)	571
Block size	128
Digest size	48
Key types	ECDSA BIP32
Algorithms	SHA384
Modes	None
Flags	Extractable

CKM_ECDSA_SHA512

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	105
Minimum key length for FIPS use (bits)	224
Minimum legacy key length for FIPS use (bits)	160
Maximum key length (bits)	571
Block size	128
Digest size	*
Key types	ECDSA BIP32
Algorithms	SHA512
Modes	None
Flags	Extractable

CKM_ECIES

NOTE This is a single part operation, so even if it is called using multi-part API, we accumulate the data (up to a maximum) and return data only on the “final” operation. That is the meaning of "Accumulating" in the table, below.

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt
Minimum key length (bits)	105
Minimum key length for FIPS use (bits)	224
Minimum legacy key length for FIPS use (bits)	160
Maximum key length (bits)	571
Block size	0
Digest size	0
Key types	ECDSA EC_MONT BIP32
Algorithms	None
Modes	None
Flags	Accumulating

CKM_EDDSA

This mechanism makes use of keys generated by "[CKM_EC_EDWARDS_KEY_PAIR_GEN](#)" on page 159 (using keys generated over Edwards curves) for EDDSA signing. The keys used by this mechanism are of type CKK_EC_EDWARDS. For SafeNet HSM, the EDDSA algorithm is compliant with "PureEDDSA" as defined in RFC 8032 and "EdDSA for more curves, July 2015".

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	0
Digest size	0
Key types	EDDSA
Algorithms	SHA512
Modes	None
Flags	Extractable

Mechanism Parameters

Mechanism parameters are optional; not using the parameters selects the PureEdDSA algorithm **ed25519**. Setting the prehashed flag (phFlag) to TRUE will select the prehashed **ed25519ph** curve variant.

```
typedef struct CK_EDDSA_PARAMS
{
    CK_BBOOL      phFlag;
    CK_ULONG      ulContextDataLen;
    CK_BYTE_PTR   pContextData;
}
```

```
CK_EDDSA_PARAMS;
```

```
CK_EDDSA_PARAMS eddsaParams;
    eddsaParams.phFlag = CK_TRUE; // Set prehashed flag to true for Ed25519ph. Setting it to
    false or not using mechanism parameters does Ed25519.
    eddsaParams.ulContextDataLen = 0; // Context length must be 0
```

```

    eddsaParams.pContextData = NULL; // Context must be NULL

CK_MECHANISM mechanism;
    mechanism.mechanism = CKM_EDDSA;
    mechanism.pParameter = &eddsaParams;
    mechanism.ulParameterLen = sizeof(eddsaParams);

C_SignInit(hSession, &mechanism, hKey); // or C_VerifyInit
// followed by C_Sign, C_SignUpdate/C_SignFinal or verify equivalents.

```

OIDs and Algorithm Identifiers for 25519 Keys

New OIDs and algorithm identifiers are as follows. Curve identifiers, including the plaintext curve names, must be ASN.1-encoded.

Edwards 25519 (sign/verify)

Curve Identifier (CKA_ECDSA_PARAMS):

- > “edwards25519” (RFC7748)
- > “Ed25519” (RFC8410)
- > 1.3.6.1.4.1.11591.15.1 (<https://www.alvestrand.no/objectid/1.3.6.1.4.1.11591.15.1.html>)

Key OIDs (wrap/unwrap):

- > 1.3.101.100 (<https://tools.ietf.org/html/draft-josefsson-pkix-eddsa-04>)
- > 1.3.101.112 (RFC8410)

Curve 25519 (ECDH)

Curve Identifier (CKA_ECDSA_PARAMS):

- > “curve25519” (RFC7748)
- > “X25519” (RFC8410)
- > 1.3.6.1.4.1.3029.1.5.1 (<http://oidref.com/1.3.6.1.4.1.3029.1.5.1>)

Key OIDs (wrap/unwrap):

- > 1.3.6.1.4.1.11591.7 (<https://tools.ietf.org/html/draft-josefsson-pkix-newcurves-00>)
- > 1.3.101.110 (RFC8410)

CKM_EDDSA_NACL

Use EDDSA keys in Networking and Cryptography Library ("salt") sign/verify operations.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	0
Digest size	0
Key types	EDDSA
Algorithms	SHA512
Modes	None
Flags	Extractable

CKM_GENERIC_SECRET_KEY_GEN

Summary

FIPS approved?	Yes
Supported functions	Generate Key
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	112
Maximum key length (bits)	4096
Block size	0
Digest size	0
Key types	None
Algorithms	None
Modes	None
Flags	None

CKM_HAS160

Summary

FIPS approved?	No
Supported functions	Digest
Minimum key length (bits)	0
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	0
Block size	64
Digest size	20
Key types	None
Algorithms	HAS160
Modes	None
Flags	Extractable Korean

CKM_KCDSA_HAS160

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	64
Digest size	20
Key types	KCDSA
Algorithms	HAS160
Modes	None
Flags	Korean

CKM_KCDSA_HAS160_NO_PAD

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	64
Digest size	20
Key types	KCDSA
Algorithms	HAS160
Modes	None
Flags	Korean

CKM_KCDSA_KEY_PAIR_GEN

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Generate Key Pair
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	0
Digest size	0
Key types	KCDSA
Algorithms	None
Modes	None
Flags	Korean

CKM_KCDSA_PARAMETER_GEN

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	0
Digest size	0
Key types	KCDSA
Algorithms	None
Modes	None
Flags	Korean

CKM_KCDSA_SHA1

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	64
Digest size	20
Key types	KCDSA
Algorithms	SHA
Modes	None
Flags	Korean

CKM_KCDSA_SHA1_NO_PAD

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	64
Digest size	20
Key types	KCDSA
Algorithms	SHA
Modes	None
Flags	Korean

CKM_KCDSA_SHA224

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	64
Digest size	28
Key types	KCDSA
Algorithms	SHA224
Modes	None
Flags	Korean

CKM_KCDSA_SHA224_NO_PAD

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	64
Digest size	28
Key types	KCDSA
Algorithms	SHA224
Modes	None
Flags	Korean

CKM_KCDSA_SHA256

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	64
Digest size	32
Key types	KCDSA
Algorithms	SHA256
Modes	None
Flags	Korean

CKM_KCDSA_SHA256_NO_PAD

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	64
Digest size	32
Key types	KCDSA
Algorithms	SHA256
Modes	None
Flags	Korean

CKM_KCDSA_SHA384

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	128
Digest size	48
Key types	KCDSA
Algorithms	SHA384
Modes	None
Flags	Korean

CKM_KCDSA_SHA384_NO_PAD

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	128
Digest size	48
Key types	KCDSA
Algorithms	SHA384
Modes	None
Flags	Korean

CKM_KCDSA_SHA512

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	128
Digest size	*
Key types	KCDSA
Algorithms	SHA512
Modes	None
Flags	Korean

CKM_KCDSA_SHA512_NO_PAD

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	128
Digest size	*
Key types	KCDSA
Algorithms	SHA512
Modes	None
Flags	Korean

CKM_KEY_WRAP_SET_OAEP

Summary

FIPS approved?	No
Supported functions	Wrap Unwrap
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	8192
Block size	0
Digest size	0
Key types	RSA
Algorithms	None
Modes	None
Flags	None

CKM_MD2

Summary

FIPS approved?	No
Supported functions	Digest
Minimum key length (bits)	0
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	0
Block size	16
Digest size	16
Key types	None
Algorithms	MD2
Modes	None
Flags	Extractable

CKM_MD2_KEY_DERIVATION

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	16
Digest size	16
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

CKM_MD5_HMAC

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	64
Digest size	16
Key types	Symmetric
Algorithms	MD5
Modes	HMAC
Flags	Extractable

CKM_MD5_HMAC_GENERAL

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	64
Digest size	16
Key types	Symmetric
Algorithms	MD5
Modes	HMAC
Flags	Extractable

CKM_MD5_KEY_DERIVATION

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	64
Digest size	16
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

CKM_NIST_PRF_KDF

Summary

FIPS approved?	Yes
Supported functions	Derive
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	112
Maximum key length (bits)	4096
Block size	0
Digest size	0
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

Usage

The CKM_NIST_PRF_KDF mechanism only supports counter mode. CKM_NIST_PRF_KDF is always allowed, whether **HSM policy 12: Allow Non-FIPS algorithms** is on or off. This mechanism can be used with the following mechanisms as the pseudorandom function:

- > AES_CMAC
- > DES3_CMAC
- > HMAC_SHA1
- > HMAC_SHA224
- > HMAC_SHA256
- > HMAC_SHA384
- > HMAC_SHA512

NIST SP 800-108 allows for some variation on what/how information is encoded and describes some fields as optional. To accommodate this, there are multiple encoding schemes you can specify, with variations on what information is included and what order the fields are arranged in. All counters and lengths are represented in big endian format. The following schemes are available:

- > LUNA_PRF_KDF_ENCODING_SCHEME_1: the **Counter** (4 bytes), **Context**, **Separator byte**, **Label**, and **Length** (4 bytes) fields are included.
- > LUNA_PRF_KDF_ENCODING_SCHEME_2: the **Counter** (4 bytes), **Context** and **Label** fields are included.
- > LUNA_PRF_KDF_ENCODING_SCHEME_3: the **Counter** (4 bytes), **Label**, **Separator byte**, **Context**, and **Length** (4 bytes) fields are included.
- > LUNA_PRF_KDF_ENCODING_SCHEME_4: the **Counter** (4 bytes), **Label** and **Context** fields are included.
- > LUNA_PRF_KDF_ENCODING_SCHEME_SCP03: the **Label**, **Separator byte**, **Length** (2 bytes), **Counter**, and **Context** fields are included.
- > LUNA_PRF_KDF_ENCODING_SCHEME_HID_KD: the **Counter**, **Label**, **Separator byte**, **Context**, and **Length** (2 bytes) fields are included.

Example

```

/* Parameter and values used with CKM_PRF_KDF and CKM_NIST_PRF_KDF. */
typedef CK_ULONG CK_KDF_PRF_TYPE;
typedef CK_ULONG CK_KDF_PRF_ENCODING_SCHEME;
/** PRF KDF schemes */
#define CK_NIST_PRF_KDF_DES3_CMAC      0x00000001
#define CK_NIST_PRF_KDF_AES_CMAC      0x00000002
#define CK_PRF_KDF_ARIA_CMAC          0x00000003
#define CK_PRF_KDF_SEED_CMAC          0x00000004
#define CK_NIST_PRF_KDF_HMAC_SHA1     0x00000005
#define CK_NIST_PRF_KDF_HMAC_SHA224   0x00000006
#define CK_NIST_PRF_KDF_HMAC_SHA256   0x00000007
#define CK_NIST_PRF_KDF_HMAC_SHA384   0x00000008
#define CK_NIST_PRF_KDF_HMAC_SHA512   0x00000009
#define CK_PRF_KDF_HMAC_RIPEMD160     0x0000000A
#define LUNA_PRF_KDF_ENCODING_SCHEME_1 0x00000000 // Counter (4 bytes) || Context || 0x00 ||
Label || Length
#define LUNA_PRF_KDF_ENCODING_SCHEME_2 0x00000001 // Counter (4 bytes) || Context || Label
#define LUNA_PRF_KDF_ENCODING_SCHEME_3 0x00000002 // Counter (4 bytes) || Label || 0x00 ||
Context || Length
#define LUNA_PRF_KDF_ENCODING_SCHEME_4 0x00000003 // Counter (4 bytes) || Label || Context
#define LUNA_PRF_KDF_ENCODING_SCHEME_SCP03 0x00000004 // Label || 0x00 || Length (2 bytes) ||
Counter (1 byte) || Context
#define LUNA_PRF_KDF_ENCODING_SCHEME_HID_KD 0x00000005 // Counter (1 byte) || Label || 0x00 ||
Context || Length (2 bytes)
typedef struct CK_KDF_PRF_PARAMS {
CK_KDF_PRF_TYPE      prfType;
CK_BYTE_PTR         pLabel;
CK_ULONG            ulLabelLen;
CK_BYTE_PTR         pContext;
CK_ULONG            ulContextLen;
CK_ULONG            ulCounter;
CK_KDF_PRF_ENCODING_SCHEME ulEncodingScheme;
} CK_PRF_KDF_PARAMS;
typedef CK_PRF_KDF_PARAMS CK_PTR CK_KDF_PRF_PARAMS_PTR;

```

CKM_PBE_MD2_DES_CBC

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	64
Block size	16
Digest size	16
Key types	None
Algorithms	None
Modes	None
Flags	None

CKM_PBE_SHA1_CAST5_CBC

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	64
Digest size	20
Key types	None
Algorithms	None
Modes	None
Flags	None

CKM_PBE_SHA1_DES2_EDE_CBC

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	64
Digest size	20
Key types	None
Algorithms	None
Modes	None
Flags	None

CKM_PBE_SHA1_DES2_EDE_CBC_OLD

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	64
Digest size	20
Key types	None
Algorithms	None
Modes	None
Flags	None

CKM_PBE_SHA1_DES3_EDE_CBC

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	192
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	192
Block size	64
Digest size	20
Key types	None
Algorithms	None
Modes	None
Flags	None

CKM_PBE_SHA1_DES3_EDE_CBC_OLD

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	192
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	192
Block size	64
Digest size	20
Key types	None
Algorithms	None
Modes	None
Flags	None

CKM_PBE_SHA1_RC2_40_CBC

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	40
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	40
Block size	64
Digest size	20
Key types	None
Algorithms	None
Modes	None
Flags	None

CKM_PBE_SHA1_RC2_128_CBC

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	64
Digest size	20
Key types	None
Algorithms	None
Modes	None
Flags	None

CKM_PBE_SHA1_RC4_40

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	40
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	40
Block size	64
Digest size	20
Key types	None
Algorithms	None
Modes	None
Flags	None

CKM_PBE_SHA1_RC4_128

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	64
Digest size	20
Key types	None
Algorithms	None
Modes	None
Flags	None

CKM_PKCS5_PBKD2

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	0
Digest size	0
Key types	None
Algorithms	None
Modes	None
Flags	None

CKM_PRF_KDF

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	0
Digest size	0
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

Usage

The CKM_NIST_PRF mechanism only supports counter mode. CKM_PRF_KDF is only available with **HSM policy 12: Allow Non-FIPS algorithms** turned on. This mechanism can be used with the following mechanisms as the pseudorandom function:

- > ARIA_CMAC
- > HMAC_RIPEMD160
- > SEED_CMAC

NIST SP 800-108 allows for some variation on what/how information is encoded and describes some fields as optional. To accommodate this, there are multiple encoding schemes you can specify, with variations on what information is included and what order the fields are arranged in. All counters and lengths are represented in big endian format. The following schemes are available:

- > LUNA_PRF_KDF_ENCODING_SCHEME_1: the **Counter** (4 bytes), **Context**, **Separator byte**, **Label**, and **Length** (4 bytes) fields are included.
- > LUNA_PRF_KDF_ENCODING_SCHEME_2: the **Counter** (4 bytes), **Context** and **Label** fields are included.

- > LUNA_PRF_KDF_ENCODING_SCHEME_3: the **Counter** (4 bytes), **Label**, **Separator byte**, **Context**, and **Length** (4 bytes) fields are included.
- > LUNA_PRF_KDF_ENCODING_SCHEME_4: the **Counter** (4 bytes), **Label** and **Context** fields are included.
- > LUNA_PRF_KDF_ENCODING_SCHEME_SCP03: the **Label**, **Separator byte**, **Length** (2 bytes), **Counter**, and **Context** fields are included.
- > LUNA_PRF_KDF_ENCODING_SCHEME_HID_KD: the **Counter**, **Label**, **Separator byte**, **Context**, and **Length** (2 bytes) fields are included.

Example

```

/* Parameter and values used with CKM_PRF_KDF and CKM_NIST_PRF_KDF. */
typedef CK_ULONG CK_KDF_PRF_TYPE;
typedef CK_ULONG CK_KDF_PRF_ENCODING_SCHEME;
/** PRF KDF schemes */
#define CK_NIST_PRF_KDF_DES3_CMAC      0x00000001
#define CK_NIST_PRF_KDF_AES_CMAC      0x00000002
#define CK_PRF_KDF_ARIA_CMAC          0x00000003
#define CK_PRF_KDF_SEED_CMAC          0x00000004
#define CK_NIST_PRF_KDF_HMAC_SHA1     0x00000005
#define CK_NIST_PRF_KDF_HMAC_SHA224   0x00000006
#define CK_NIST_PRF_KDF_HMAC_SHA256   0x00000007
#define CK_NIST_PRF_KDF_HMAC_SHA384   0x00000008
#define CK_NIST_PRF_KDF_HMAC_SHA512   0x00000009
#define CK_PRF_KDF_HMAC_RIPEMD160     0x0000000A
#define LUNA_PRF_KDF_ENCODING_SCHEME_1 0x00000000 // Counter (4 bytes) || Context || 0x00 ||
Label || Length
#define LUNA_PRF_KDF_ENCODING_SCHEME_2 0x00000001 // Counter (4 bytes) || Context || Label
#define LUNA_PRF_KDF_ENCODING_SCHEME_3 0x00000002 // Counter (4 bytes) || Label || 0x00 ||
Context || Length
#define LUNA_PRF_KDF_ENCODING_SCHEME_4 0x00000003 // Counter (4 bytes) || Label || Context
#define LUNA_PRF_KDF_ENCODING_SCHEME_SCP03 0x00000004 // Label || 0x00 || Length (2 bytes) ||
Counter (1 byte) || Context
#define LUNA_PRF_KDF_ENCODING_SCHEME_HID_KD 0x00000005 // Counter (1 byte) || Label || 0x00 ||
Context || Length (2 bytes)
typedef struct CK_KDF_PRF_PARAMS {
CK_KDF_PRF_TYPE      prfType;
CK_BYTE_PTR         pLabel;
CK_ULONG            ulLabelLen;
CK_BYTE_PTR         pContext;
CK_ULONG            ulContextLen;
CK_ULONG            ulCounter;
CK_KDF_PRF_ENCODING_SCHEME ulEncodingScheme;
} CK_PRF_KDF_PARAMS;
typedef CK_PRF_KDF_PARAMS CK_PTR CK_KDF_PRF_PARAMS_PTR;

```

CKM_RC2_CBC

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	1024
Block size	8
Digest size	0
Key types	RC2
Algorithms	RC2
Modes	CBC
Flags	Extractable

CKM_RC2_CBC_PAD

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	1024
Block size	8
Digest size	0
Key types	RC2
Algorithms	RC2
Modes	CBC_PAD
Flags	Extractable

CKM_RC2_ECB

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	1024
Block size	8
Digest size	0
Key types	RC2
Algorithms	RC2
Modes	ECB
Flags	Extractable

CKM_RC2_KEY_GEN

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	1024
Block size	0
Digest size	0
Key types	RC2
Algorithms	None
Modes	None
Flags	None

CKM_RC2_MAC

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	1024
Block size	8
Digest size	0
Key types	RC2
Algorithms	RC2
Modes	MAC
Flags	Extractable

CKM_RC2_MAC_GENERAL

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	1024
Block size	8
Digest size	0
Key types	RC2
Algorithms	RC2
Modes	MAC
Flags	Extractable

CKM_RC4

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	0
Digest size	0
Key types	RC4
Algorithms	RC4
Modes	STREAM
Flags	Extractable

CKM_RC4_KEY_GEN

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2048
Block size	0
Digest size	0
Key types	RC4
Algorithms	None
Modes	None
Flags	None

CKM_RC5_CBC

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2040
Block size	8
Digest size	0
Key types	RC5
Algorithms	RC5
Modes	CBC
Flags	Extractable

CKM_RC5_CBC_PAD

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2040
Block size	8
Digest size	0
Key types	RC5
Algorithms	RC5
Modes	CBC_PAD
Flags	Extractable

CKM_RC5_ECB

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2040
Block size	8
Digest size	0
Key types	RC5
Algorithms	RC5
Modes	ECB
Flags	Extractable

CKM_RC5_KEY_GEN

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2040
Block size	0
Digest size	0
Key types	RC5
Algorithms	None
Modes	None
Flags	None

CKM_RC5_MAC

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2040
Block size	8
Digest size	0
Key types	RC5
Algorithms	RC5
Modes	MAC
Flags	Extractable

CKM_RC5_MAC_GENERAL

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	64
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	2040
Block size	8
Digest size	0
Key types	RC5
Algorithms	RC5
Modes	MAC
Flags	Extractable

CKM_RSA_FIPS_186_3_AUX_PRIME_KEY_PAIR_GEN

Summary

FIPS approved?	Yes
Supported functions	Generate Key Pair
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	4096
Block size	0
Digest size	0
Key types	RSA
Algorithms	None
Modes	None
Flags	None

CKM_RSA_FIPS_186_3_PRIME_KEY_PAIR_GEN

Summary

FIPS approved?	Yes
Supported functions	Generate Key Pair
Minimum key length (bits)	2048
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	2048
Maximum key length (bits)	4096
Block size	0
Digest size	0
Key types	RSA
Algorithms	None
Modes	None
Flags	None

CKM_RSA_PKCS

Summary

FIPS approved?	Yes
Supported functions	Sign Verify Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	0
Digest size	0
Key types	RSA
Algorithms	None
Modes	None
Flags	None

CKM_RSA_PKCS_KEY_PAIR_GEN

Summary

FIPS approved?	No
Supported functions	Generate Key Pair
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	8192
Block size	0
Digest size	0
Key types	RSA
Algorithms	None
Modes	None
Flags	None

CKM_RSA_PKCS_OAEP

The RSA PKCS OAEP mechanism can now use a supplied hashing mechanism. Previously RSA OAEP would always use SHA1 and returned an error if another was attempted.

With current firmware, PKCS#11 API and ckdemo now accept a new mechanism.

Allowed mechanisms are:

CKM_SHA1

CKM_SHA224

CKM_SHA256

CKM_SHA384

CKM_SHA512

0 (use the firmware's default engine, which is currently SHA1)

In ckdemo menu option 98 has a new value 17 - OAEP Hash Params, which can be set to use either default (CKM_SHA1) or selectable. When it is set to selectable the user is prompted for a hash mechanism when using the OAEP mechanism.

Summary

FIPS approved?	Yes
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	0
Digest size	0
Key types	RSA
Algorithms	None
Modes	None
Flags	None

CKM_RSA_PKCS_PSS

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	0
Digest size	0
Key types	RSA
Algorithms	None
Modes	None
Flags	None PSS

CKM_RSA_X_509

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	8192
Block size	0
Digest size	0
Key types	RSA
Algorithms	None
Modes	None
Flags	None

CKM_RSA_X9_31

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	0
Digest size	0
Key types	RSA
Algorithms	None
Modes	None
Flags	Extractable X9.31

CKM_RSA_X9_31_KEY_PAIR_GEN

Summary

FIPS approved?	No
Supported functions	Generate Key Pair
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	8192
Block size	0
Digest size	0
Key types	RSA
Algorithms	None
Modes	None
Flags	X9.31

CKM_RSA_X9_31_NON_FIPS

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	8192
Block size	0
Digest size	0
Key types	RSA
Algorithms	None
Modes	None
Flags	Extractable X9.31 Non-FIPS X9.31

CKM_SEED_CBC

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	16
Digest size	0
Key types	SEED
Algorithms	SEED
Modes	CBC
Flags	Extractable Korean

CKM_SEED_CBC_PAD

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	16
Digest size	0
Key types	SEED
Algorithms	SEED
Modes	CBC_PAD
Flags	Extractable Korean

CKM_SEED_CMAC

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	16
Digest size	0
Key types	SEED
Algorithms	SEED
Modes	MAC
Flags	Extractable Korean CMAC

CKM_SEED_CMACE_GENERAL

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	16
Digest size	0
Key types	SEED
Algorithms	SEED
Modes	MAC
Flags	Extractable Korean CMACE

CKM_SEED_CTR

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	16
Digest size	0
Key types	SEED
Algorithms	SEED
Modes	CTR
Flags	Extractable Korean

CKM_SEED_ECB

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt Wrap Unwrap
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	16
Digest size	0
Key types	SEED
Algorithms	SEED
Modes	ECB
Flags	Extractable Korean

CKM_SEED_KEY_GEN

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	0
Digest size	0
Key types	SEED
Algorithms	None
Modes	None
Flags	Korean

CKM_SEED_MAC

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	16
Digest size	0
Key types	SEED
Algorithms	SEED
Modes	MAC
Flags	Extractable Korean

CKM_SEED_MAC_GENERAL

NOTE The SEED and ARIA and KCDSA mechanisms are available on your HSM if Korean Algorithms are enabled.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	16
Digest size	0
Key types	SEED
Algorithms	SEED
Modes	MAC
Flags	Extractable Korean

CKM_SHA_1

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	Yes
Supported functions	Digest
Minimum key length (bits)	0
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	0
Maximum key length (bits)	0
Block size	64
Digest size	20
Key types	None
Algorithms	SHA
Modes	None
Flags	Extractable

CKM_SHA_1_HMAC

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	112
Minimum legacy key length for FIPS use (bits)	80
Maximum key length (bits)	4096
Block size	64
Digest size	20
Key types	Symmetric
Algorithms	SHA
Modes	HMAC
Flags	Extractable

CKM_SHA_1_HMAC_GENERAL

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	112
Minimum legacy key length for FIPS use (bits)	80
Maximum key length (bits)	4096
Block size	64
Digest size	20
Key types	Symmetric
Algorithms	SHA
Modes	HMAC
Flags	Extractable

CKM_SHA1_EDDSA

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	64
Digest size	20
Key types	EDDSA
Algorithms	SHA
Modes	None
Flags	Extractable

CKM_SHA1_EDDSA_NACL

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	64
Digest size	20
Key types	EDDSA
Algorithms	SHA
Modes	None
Flags	Extractable

CKM_SHA1_KEY_DERIVATION

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	64
Digest size	20
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

CKM_SHA1_RSA_PKCS

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	64
Digest size	20
Key types	RSA
Algorithms	SHA
Modes	None
Flags	Extractable

CKM_SHA1_RSA_PKCS_PSS

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	64
Digest size	20
Key types	RSA
Algorithms	SHA
Modes	None
Flags	Extractable PSS

CKM_SHA1_RSA_X9_31

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	64
Digest size	20
Key types	RSA
Algorithms	SHA
Modes	None
Flags	Extractable X9.31

CKM_SHA1_RSA_X9_31_NON_FIPS

NOTE The flags MPE_NO_SIGN and MPE_NO_WRAP are assigned to the SHA1 mechanisms. When the HSM policy “Allow NonFIPS Algorithms” is disabled, mechanisms with the MPE_NO_SIGN flag *are not* allowed to sign data, and mechanisms with the MPE_NO_WRAP flag *are not* allowed to wrap objects. When the policy is enabled, these mechanisms *are* allowed to sign data and wrap objects respectively.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	8192
Block size	64
Digest size	20
Key types	RSA
Algorithms	SHA
Modes	None
Flags	Extractable X9.31 Non-FIPS X9.31

CKM_SHA224

Summary

FIPS approved?	Yes
Supported functions	Digest
Minimum key length (bits)	0
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	0
Maximum key length (bits)	0
Block size	64
Digest size	28
Key types	None
Algorithms	SHA224
Modes	None
Flags	Extractable

CKM_SHA224_EDDSA

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	64
Digest size	28
Key types	EDDSA
Algorithms	SHA224
Modes	None
Flags	Extractable

CKM_SHA224_EDDSA_NACL

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	64
Digest size	28
Key types	EDDSA
Algorithms	SHA224
Modes	None
Flags	Extractable

CKM_SHA224_HMAC

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	112
Minimum legacy key length for FIPS use (bits)	80
Maximum key length (bits)	4096
Block size	64
Digest size	28
Key types	Symmetric
Algorithms	SHA224
Modes	HMAC
Flags	Extractable

CKM_SHA224_HMAC_GENERAL

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	112
Minimum legacy key length for FIPS use (bits)	80
Maximum key length (bits)	4096
Block size	64
Digest size	28
Key types	Symmetric
Algorithms	SHA224
Modes	HMAC
Flags	Extractable

CKM_SHA224_KEY_DERIVATION

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	64
Digest size	28
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

CKM_SHA224_RSA_PKCS

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	64
Digest size	28
Key types	RSA
Algorithms	SHA224
Modes	None
Flags	Extractable

CKM_SHA224_RSA_PKCS_PSS

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	512
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	64
Digest size	28
Key types	RSA
Algorithms	SHA224
Modes	None
Flags	Extractable PSS

CKM_SHA224_RSA_X9_31

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	64
Digest size	28
Key types	RSA
Algorithms	SHA224
Modes	None
Flags	Extractable X9.31

CKM_SHA224_RSA_X9_31_NON_FIPS

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	8192
Block size	64
Digest size	28
Key types	RSA
Algorithms	SHA224
Modes	None
Flags	Extractable X9.31 Non-FIPS X9.31

CKM_SHA256

Summary

FIPS approved?	Yes
Supported functions	Digest
Minimum key length (bits)	0
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	0
Maximum key length (bits)	0
Block size	64
Digest size	32
Key types	None
Algorithms	SHA256
Modes	None
Flags	Extractable

CKM_SHA256_EDDSA

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	64
Digest size	32
Key types	EDDSA
Algorithms	SHA256
Modes	None
Flags	Extractable

CKM_SHA256_EDDSA_NACL

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	128
Digest size	48
Key types	EDDSA
Algorithms	SHA384
Modes	None
Flags	Extractable

CKM_SHA256_HMAC

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	112
Minimum legacy key length for FIPS use (bits)	80
Maximum key length (bits)	4096
Block size	64
Digest size	32
Key types	Symmetric
Algorithms	SHA256
Modes	HMAC
Flags	Extractable

CKM_SHA256_HMAC_GENERAL

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	112
Minimum legacy key length for FIPS use (bits)	80
Maximum key length (bits)	4096
Block size	64
Digest size	32
Key types	Symmetric
Algorithms	SHA256
Modes	HMAC
Flags	Extractable

CKM_SHA256_KEY_DERIVATION

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	64
Digest size	32
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

CKM_SHA256_RSA_PKCS

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	64
Digest size	32
Key types	RSA
Algorithms	SHA256
Modes	None
Flags	Extractable

CKM_SHA256_RSA_PKCS_PSS

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	512
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	64
Digest size	32
Key types	RSA
Algorithms	SHA256
Modes	None
Flags	Extractable PSS

CKM_SHA256_RSA_X9_31

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	64
Digest size	32
Key types	RSA
Algorithms	SHA256
Modes	None
Flags	Extractable X9.31

CKM_SHA256_RSA_X9_31_NON_FIPS

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	8192
Block size	64
Digest size	32
Key types	RSA
Algorithms	SHA256
Modes	None
Flags	Extractable X9.31 Non-FIPS X9.31

CKM_SHA384

Summary

FIPS approved?	Yes
Supported functions	Digest
Minimum key length (bits)	0
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	0
Maximum key length (bits)	0
Block size	128
Digest size	48
Key types	None
Algorithms	SHA384
Modes	None
Flags	Extractable

CKM_SHA384_EDDSA

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	128
Digest size	48
Key types	EDDSA
Algorithms	SHA384
Modes	None
Flags	Extractable

CKM_SHA384_EDDSA_NACL

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	128
Digest size	48
Key types	EDDSA
Algorithms	SHA384
Modes	None
Flags	Extractable

CKM_SHA384_HMAC

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	112
Minimum legacy key length for FIPS use (bits)	80
Maximum key length (bits)	4096
Block size	128
Digest size	48
Key types	Symmetric
Algorithms	SHA384
Modes	HMAC
Flags	Extractable

CKM_SHA384_HMAC_GENERAL

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	112
Minimum legacy key length for FIPS use (bits)	80
Maximum key length (bits)	4096
Block size	128
Digest size	48
Key types	Symmetric
Algorithms	SHA384
Modes	HMAC
Flags	Extractable

CKM_SHA384_KEY_DERIVATION

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	128
Digest size	48
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

CKM_SHA384_RSA_PKCS

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	128
Digest size	48
Key types	RSA
Algorithms	SHA384
Modes	None
Flags	Extractable

CKM_SHA384_RSA_PKCS_PSS

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	512
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	128
Digest size	48
Key types	RSA
Algorithms	SHA384
Modes	None
Flags	Extractable PSS

CKM_SHA384_RSA_X9_31

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	128
Digest size	48
Key types	RSA
Algorithms	SHA384
Modes	None
Flags	Extractable X9.31

CKM_SHA384_RSA_X9_31_NON_FIPS

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	8192
Block size	128
Digest size	48
Key types	RSA
Algorithms	SHA384
Modes	None
Flags	Extractable X9.31 Non-FIPS X9.31

CKM_SHA512

Summary

FIPS approved?	Yes
Supported functions	Digest
Minimum key length (bits)	0
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	0
Maximum key length (bits)	0
Block size	128
Digest size	*
Key types	None
Algorithms	SHA512
Modes	None
Flags	Extractable

CKM_SHA512_EDDSA

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	128
Digest size	*
Key types	EDDSA
Algorithms	SHA512
Modes	None
Flags	Extractable

CKM_SHA512_EDDSA_NACL

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	256
Block size	128
Digest size	*
Key types	EDDSA
Algorithms	SHA512
Modes	None
Flags	Extractable

CKM_SHA512_HMAC

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	112
Minimum legacy key length for FIPS use (bits)	80
Maximum key length (bits)	4096
Block size	128
Digest size	*
Key types	Symmetric
Algorithms	SHA512
Modes	HMAC
Flags	Extractable

CKM_SHA512_HMAC_GENERAL

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	112
Minimum legacy key length for FIPS use (bits)	80
Maximum key length (bits)	4096
Block size	128
Digest size	*
Key types	Symmetric
Algorithms	SHA512
Modes	HMAC
Flags	Extractable

CKM_SHA512_KEY_DERIVATION

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	128
Digest size	*
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

CKM_SHA512_RSA_PKCS

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	256
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	128
Digest size	*
Key types	RSA
Algorithms	SHA512
Modes	None
Flags	Extractable

CKM_SHA512_RSA_PKCS_PSS

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	128
Digest size	*
Key types	RSA
Algorithms	SHA512
Modes	None
Flags	Extractable PSS

CKM_SHA512_RSA_X9_31

Summary

FIPS approved?	Yes
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	2048
Minimum legacy key length for FIPS use (bits)	1024
Maximum key length (bits)	8192
Block size	128
Digest size	*
Key types	RSA
Algorithms	SHA512
Modes	None
Flags	Extractable X9.31

CKM_SHA512_RSA_X9_31_NON_FIPS

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	8192
Block size	128
Digest size	*
Key types	RSA
Algorithms	SHA512
Modes	None
Flags	Extractable X9.31 Non-FIPS X9.31

CKM_SM3

SM3 is a hash function published by the Chinese Commercial Cryptography Administration Office for the use of electronic authentication service system. The design of SM3 builds upon the design of the SHA-2 hash function, but introduces additional strengthening features. For SafeNet Luna PCIe HSMs, the available mechanisms are CKM_SM3, the hash function, and CKM_SM3_KEY_DERIVATION, and CKM_HMAC_SM3.

Summary

FIPS approved?	No
Supported functions	Digest
Minimum key length (bits)	0
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	0
Block size	64
Digest size	32
Key types	None
Algorithms	SM3
Modes	None
Flags	None

CKM_SM3_HMAC

SM3 is a hash function published by the Chinese Commercial Cryptography Administration Office for the use of electronic authentication service system. The design of SM3 builds upon the design of the SHA-2 hash function, but introduces additional strengthening features. For SafeNet Luna PCIe HSMs, the available mechanisms are CKM_SM3, the hash function, and CKM_SM3_KEY_DERIVATION, and CKM_SM3_HMAC.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	64
Digest size	32
Key types	Symmetric
Algorithms	SM3
Modes	HMAC
Flags	None

CKM_SM3_HMAC_GENERAL

SM3 is a hash function published by the Chinese Commercial Cryptography Administration Office for the use of electronic authentication service system. The design of SM3 builds upon the design of the SHA-2 hash function, but introduces additional strengthening features. For SafeNet Luna PCIe HSMs, the available mechanisms are CKM_SM3, the hash function, and CKM_SM3_KEY_DERIVATION, and CKM_SM3_HMAC.

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	64
Digest size	32
Key types	Symmetric
Algorithms	SM3
Modes	HMAC
Flags	None

CKM_SM3_KEY_DERIVATION

SM3 is a hash function published by the Chinese Commercial Cryptography Administration Office for the use of electronic authentication service system. The design of SM3 builds upon the design of the SHA-2 hash function, but introduces additional strengthening features. For SafeNet Luna PCIe HSMs, the available mechanisms are CKM_SM3, the hash function, and CKM_SM3_KEY_DERIVATION, and CKM_HMAC_SM3.

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	64
Digest size	32
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

CKM_SSL3_KEY_AND_MAC_DERIVE

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	384
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	384
Block size	0
Digest size	0
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

CKM_SSL3_MASTER_KEY_DERIVE

Summary

FIPS approved?	No
Supported functions	Derive
Minimum key length (bits)	384
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	384
Block size	0
Digest size	0
Key types	Symmetric
Algorithms	None
Modes	None
Flags	None

CKM_SSL3_MD5_MAC

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	128
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	128
Block size	64
Digest size	16
Key types	Symmetric
Algorithms	MD5
Modes	HMAC
Flags	Extractable

CKM_SSL3_PRE_MASTER_KEY_GEN

Summary

FIPS approved?	No
Supported functions	Generate Key
Minimum key length (bits)	384
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	384
Block size	0
Digest size	0
Key types	None
Algorithms	None
Modes	None
Flags	None

CKM_SSL3_SHA1_MAC

Summary

FIPS approved?	No
Supported functions	Sign Verify
Minimum key length (bits)	160
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	160
Block size	64
Digest size	20
Key types	Symmetric
Algorithms	SHA
Modes	HMAC
Flags	Extractable

CKM_X9_42_DH_DERIVE

Summary

FIPS approved?	Yes
Supported functions	Derive
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	2048
Maximum key length (bits)	4096
Block size	0
Digest size	0
Key types	X9_42_DH
Algorithms	None
Modes	None
Flags	None

CKM_X9_42_DH_HYBRID_DERIVE

Summary

FIPS approved?	Yes
Supported functions	Derive
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	2048
Maximum key length (bits)	4096
Block size	0
Digest size	0
Key types	X9_42_DH
Algorithms	None
Modes	None
Flags	None

CKM_X9_42_DH_KEY_PAIR_GEN

Summary

FIPS approved?	Yes
Supported functions	Generate Key Pair
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	2048
Maximum key length (bits)	4096
Block size	0
Digest size	0
Key types	X9_42_DH
Algorithms	None
Modes	None
Flags	None

CKM_X9_42_DH_PARAMETER_GEN

Summary

FIPS approved?	Yes
Supported functions	Generate Key
Minimum key length (bits)	1024
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	2048
Maximum key length (bits)	4096
Block size	0
Digest size	0
Key types	X9_42_DH
Algorithms	None
Modes	None
Flags	None

CKM_XOR_BASE_AND_DATA_W_KDF

Summary

FIPS approved?	No
Supported functions	Encrypt Decrypt
Minimum key length (bits)	8
Minimum key length for FIPS use (bits)	N/A
Minimum legacy key length for FIPS use (bits)	N/A
Maximum key length (bits)	4096
Block size	0
Digest size	0
Key types	Symmetric
Algorithms	None
Modes	OFB
Flags	None

CHAPTER 5: Using the SafeNet SDK

This chapter describes how to use the SDK to develop applications that exercise the HSM. It contains the following topics:

- > "Libraries and Applications" below
- > "Application IDs" on page 314
- > "Named Curves and User-Defined Parameters" on page 318
- > "Supported ECC Curves" on page 325
- > "Capability and Policy Configuration Control Using the SafeNet API" on page 328
- > "Connection Timeout" on page 332

Libraries and Applications

This section explains how to make the Chrystoki library available to the other components of the SafeNet Software Development Kit.

An application has no knowledge of which library is to be loaded nor does the application know the library's location. For these reasons, a special scheme must be employed to tell the application, while it is running, where to find the library. The next paragraphs describe how applications connect to Chrystoki.

SafeNet SDK Applications General Information

All applications provided in SafeNet Luna PCIe HSM Software Development Kit have been compiled with a component called CkBridge, which uses a configuration file to find the library it is intended to load. Ckbridge first uses the environment variable "ChrystokiConfigurationPath" to locate the corresponding configuration file. If this environment variable is not set, it attempts to locate the configuration file in a default location depending on the product platform (/etc on Unix, and c:\Program Files\SafeNet\LunaClient on Windows).

Configuration files differ from one platform to the next - refer to the appropriate sub-section for the operating system and syntax applicable to your development platform.

Windows

In Windows, an initialization file called **crystoki.ini** specifies which library is to be loaded. The syntax of this file is standard to Windows.

The following example shows proper configuration files for Windows:

```
[Chrystoki2]
LibNT=C:\Program Files\SafeNet\LunaClient\cryptoki.dll
[LunaSA Client]
SSLConfigFile=C:\Program Files\SafeNet\LunaClient\openssl.cnf
ReceiveTimeout=20000
NetClient=1
ServerCAFile=C:\Program Files\SafeNet\LunaClient\cert\server\CAFile.pem
ClientCertFile=C:\Program Files\SafeNet\LunaClient\cert\client\ClientNameCert.pem
```

```
ClientPrivKeyFile=C:\Program Files\SafeNet\LunaClient\cert\client\ClientNameKey.pem
[Luna]
DefaultTimeOut=500000
PEDTimeout1=100000
PEDTimeout2=200000
PEDTimeout3=10000
[CardReader]
RemoteCommand=1
```

CAUTION! Never insert TAB characters into the `crystoki.ini` (Windows) or `chrystoki.conf` (UNIX) file.

UNIX

In UNIX, a configuration file called "Chrystoki.conf" is used to guide CkBridge in finding the appropriate library.

The configuration file is a regular text file with a special format. It is made up of a number of sections, each section containing one or multiple entries. The following example shows a typical UNIX configuration file:

```
Chrystoki2 =
{
LibUNIX=/usr/lib/libCryptoki2.so;
}
Luna = {
DefaultTimeOut=500000;
PEDTimeout1=100000;
PEDTimeout2=200000;
PEDTimeout3=10000;
KeypairGenTimeOut=2700000;
CloningCommandTimeOut=300000;
}
CardReader = {
RemoteCommand=1;
}
LunaSA Client = {
NetClient = 1;
ServerCAFile = /usr/safenet/lunaclient/cert/server/CAFile.pem;
ClientCertFile = /usr/safenet/lunaclient/cert/client/ClientNameCert.pem;
ClientPrivKeyFile = /usr/safenet/lunaclient/cert/client/ClientNameKey.pem;
SSLConfigFile = /usr/safenet/lunaclient/bin/openssl.cnf;
ReceiveTimeout = 20000;
}
```

The shared object "libcryptoki2.so" is a library supporting version 2.2.0 of the PKCS#11 standard.

CAUTION! Never insert TAB characters into the `crystoki.ini` (Windows) or `crystoki.conf` (UNIX) file.

Compiler Tools

Tools used for SafeNet development are platform specific tools/development environments, where applicable (e.g., Visual C++ on Windows, or Workshop on Solaris). Current version information is provided in the Customer Release Notes.

NOTE Contact SafeNet for information about the availability of newer versions of compilers.

Using CKlog

SafeNet Software Development Kit provides a facility which can record all interactions between an application and the PKCS#11-compliant library. It allows a developer to debug an application by viewing what the library receives.

This tool is known as the Cryptoki Logging Facility or cklog. Cklog is a shim library that an application accesses when seeking our PKCS#11 library. When cklog receives a call it does not service the request. Instead, it logs the call to a file and passes the request to the originally intended library.

To configure CkLog:

Perform these steps:

1. Direct the application to use the cklog library instead of the regular Chrystoki library. Do this by modifying the configuration file to instruct CkBridge to load the Cklog library.

Windows

```
[Chrystoki2]
LibNT=c:\Program Files\SafeNet\LunaClient\cklog201.dll
```

Linux/UNIX

```
Chrystoki2 =
{
LibUNIX=/usr/lib/libcklog2.so;
```

2. Instruct the cklog library where to access the regular cryptoki library.

Windows

```
[CkLog2]
LibNT=c:\Program Files\SafeNet\LunaClient\cryptoki.dll
```

Linux/UNIX

```
CkLog2 =
{
LibUNIX=/usr/lib/libCryptoki2.so;
}
```

3. Add appropriate entries to the CkLog2 section for the desired level of operation. See the examples and explanations of entries, below.

Windows Example

The following example shows a typical initialization file under Windows where cklog is in use:

```
[Chrystoki2]
LibNT=c:\Program Files\SafeNet\LunaClient\cklog201.dll
[CkLog2]
LibNT=c:\Program Files\SafeNet\LunaClient\cryptoki.dll
Enabled=1
File=c:\Program Files\SafeNet\LunaClient\cklog2.txt
Error=c:\Program Files\SafeNet\LunaClient\error2.txt
NewFormat=1
LoggingMask=ALL_FUNC
```

UNIX Example

The following example shows a typical configuration file under UNIX where cklog is in use:

```

Chrystoki2 =
{
LibUNIX=/usr/lib/libcklog2.so;
}
CkLog2 =
{
LibUNIX=/usr/lib/libCryptoki2.so;
Enabled=1;
File=/tmp/cklog.txt;
Error=/tmp/error.txt;
NewFormat=1;
LoggingMask=ALL_FUNC;
}

```

Here are descriptions of entries that might be applicable:

- > LibNT - references to a Cryptoki library for Windows.
- > LibUNIX - references to a Cryptoki library for UNIX (meaning Solaris, Linux, and AIX).
- > Enabled - 0 or 1. Allows turning the logging facility off or on.
- > File - references the file to which the requests should be logged.
- > Error - references a file where the logging facility can record fatal errors.
- > NewFormat - 0 or 1 disables/enables a more compact output format, which is the format preferred by SafeNet Customer Support

Selective Logging

When logging is turned on, all functions are logged, by default. If you wish to restrict logging to particular functions of interest only, you can edit the “LoggingMask=” parameter in the `crystoki.ini` [Windows] or `Chrystoki.conf` [UNIX] file to include flags for the desired logging.

LoggingMask= Flags

Here is the list of possible flags for `cklog`:

Flag	Description
GEN_FUNCS	General functions
SLOT_TOKEN_FUNC	Slot/Token related functions
SESSION_FUNC	Session related functions
OBJ_MNGMNT_FUNC	Object Management functions
ENC_DEC_FUNC	Encrypt/Decrypt related functions
DIGEST_FUNC	Digest Related functions
SIGN_VERIFY_FUNC	Signing/Verifying related functions
KEY_MNGMNT_FUNC	Key Management related functions

Flag	Description
MISC_FUNC	Misc functions
CHRYSALIS_FUNC	SafeNet Extensions functions
ALL_FUNC	All functions logged;

You can mix and match any or all of the flags, using the “|” operator. For example, the following:
 LoggingMask=GEN_FUNC | SLOT_TOKEN_FUNC | ENC_DEC_FUNC | SIGN_VERIFY_FUNC;
 would be valid.

NOTE You can use the flags in any order. Using the ALL_FUNC flag overrides any other flag.
 If you have the “LoggingMask=” parameter, with NO flags set, then nothing is logged. If logging capability is enabled (cklog), but there is no “LoggingMask=” line, then default behavior prevails and everything is logged.

Application IDs

Within Chrystoki, each application has an application ID, a 64-bit integer, normally specified in two 32-bit parts. When an application invokes **C_Initialize**, the Chrystoki library automatically generates a default application ID. The default value is based on the application's process ID, so different applications will always have different application IDs. The application ID is also associated with each session created by the application.

Shared Login State and Application IDs

PKCS#11 specifies that sessions within an application (a single address space and all threads that execute within it) share a login state, meaning that if one session is logged in, all are logged in. If one logs out, all are logged out. Thus, if process A spawns multiple threads, and all of those threads open sessions on Token #1, then all of those sessions share a login state. If process B also has sessions open on Token #1, they are independent from the sessions of process A. The login state of process B sessions does not affect process A sessions, unless they conflict with one another (e.g. process A logs in as USER when process B is already logged in as SO).

Within Chrystoki and SafeNet tokens, login states are shared by sessions with the same application ID. This means that sessions within an application share a login state, but sessions across separate applications do not. However, Chrystoki does provides functionality allowing applications to alter their application IDs, so that separate applications can share a login state.

CAUTION! The ability to share login states through the use of application IDs is a legacy feature. It can eliminate the need for repeated PED authentication across multiple applications, but this is not ideal for security reasons. To avoid these risks, it is recommended to use auto-activation in conjunction with a PED challenge password instead (see "[Activation and Auto-activation on PED-Authenticated Partitions](#)" on page 1 in the *Administration Guide*).

To change application IDs manually using the LunaCM **appid** command, see "[appid](#)" on page 1 in the *LunaCM Reference Guide*.

Why Share Login State Between Applications?

For most applications, this is unnecessary. If an application consists of a single perpetual process, unshared session states are sufficient. If the application supports multiple, separately-validated processes, unshared session states are also sufficient. Generally, applications that validate (login) separately are more secure.

It is only necessary to share login state between processes if *all* of the following conditions are true:

- > the application designer wants to require only one login action by the user
- > the application consists of multiple processes, each with their own sessions
- > the system uses SafeNet CA3 tokens

The SafeNet CA3 token provides FIPS 140-1 level 3 security by using a separate port for password entry (where PINs take the form of special data keys). Use of these keys prevents an application from caching a password and using it to log in with multiple sessions. To log in to separate processes simultaneously, login state between those processes must be shared.

Login State Sharing Overview

The simplest form of the Chrystoki state-sharing functionality is the **CA_SetApplicationID** function. This function should be invoked after **C_Initialize**, but before any sessions are opened. Two separate applications can use this function to set their application IDs to the same value, and thus allow them to share login states between their sessions.

Alternatively, set the **AppIdMajor** and **AppIdMinor** fields in the Misc section of the Chrystoki configuration file. This causes default application IDs for all applications to be generated from these fields, rather than from each application's process ID. When these fields are set, all applications on a host system will share login state between their sessions, unless individual applications use the **CA_SetApplicationID** function.

Example

A sample configuration file (**crystoki.ini** for Windows) using explicit application IDs is duplicated here:

```
[Chrystoki2]
LibNT=D:\Program Files\SafeNet\LunaClient\cryptoki.dll
[Luna]
DefaultTimeOut=500000
PEDTimeout1=100000
PEDTimeout2=200000
[CardReader]
RemoteCommand=1
[Misc]
AppIdMajor=2
AppIdMinor=4
```

Problems may still arise. When all sessions of a particular application ID are closed, that application ID reverts to a dormant state. When another session for that application ID is created, the application ID is recreated, but always in the logged-out state, regardless of the state it was in when it went dormant.

For example, consider an application where a parent process sets its application ID, opens a session, logs the session in, then closes the session and terminates. Several child processes then set their application IDs, open sessions and try to use them. However, since the application ID went dormant when the parent process closed its session, the child processes find their sessions logged out. The logged-in state of the parent process's session was lost when it closed its session.

The **CA_OpenApplicationID** function can ensure that the login state of an application ID is maintained, even when no sessions belonging to that application ID exist. When **CA_OpenApplicationID** is invoked, the application ID is tagged so that it never goes dormant, even if no open sessions exist.

NOTE Running **CA_OpenApplication_ID** does not set the application ID for the current process. You must first explicitly run **CA_SetApplicationID** to do this.

Login State Sharing Functions

Use the following functions to configure and manage login state sharing:

CA_SetApplicationID

```
CK_RV CK_ENTRY CA_SetApplicationID(
    CK_ULONG ulHigh,
    CK_ULONG ulLow
);
```

The **CA_SetApplicationID** function allows an application to set its own application ID, rather than letting the application ID be generated automatically from the application's process ID. **CA_SetApplicationID** should be invoked after **C_Initialize**, but before any session manipulation functions are invoked. If **CA_SetApplicationID** is invoked after sessions have been opened, results will be unpredictable.

CA_SetApplicationID always returns **CKR_OK**.

CA_OpenApplicationID

```
CK_RV CK_ENTRY CA_OpenApplicationID(
    CK_SLOT_ID slotID,
    CK_ULONG ulHigh,
    CK_ULONG ulLow
);
```

The **CA_OpenApplicationID** function forces a given application ID on a given token to remain active, even when all sessions belonging to the application ID have been closed. Normally, an application ID on a token goes dormant when the last session that belongs to the application ID is closed. When an application ID goes dormant, login state is lost, so when a new session is created within the application ID, it starts in the logged-out state. However, if **CA_OpenApplicationID** is used, the application ID is prevented from going dormant, so login state is maintained even when all sessions for an application ID are closed.

NOTE Running **CA_OpenApplication_ID** does not set the application ID for the current process. You must first explicitly run **CA_SetApplicationID** to do this.

CA_OpenApplicationID can return **CKR_SLOT_ID_INVALID** or **CKR_TOKEN_NOT_PRESENT**.

CA_CloseApplicationID

```
CK_RV CK_ENTRY CA_CloseApplicationID(
    CK_SLOT_ID slotID,
    CK_ULONG ulHigh,
    CK_ULONG ulLow
);
```

The **CA_CloseApplicationID** function removes the property of an application ID that prevents it from going dormant. **CA_CloseApplicationID** also closes any open sessions owned by the given application ID. Thus, when **CA_CloseApplicationID** returns, all open sessions owned by the given application ID have been closed and the application ID has gone dormant.

CA_CloseApplicationID can return **CKR_SLOT_ID_INVALID** or **CKR_TOKEN_NOT_PRESENT**.

Application ID Examples

The following code fragments show how two separate applications might share a single application ID:

```
app 1:      app 2:
C_Initialize()
CA_SetApplicationID(3,4)
C_OpenSession()
C_Login()

      C_Initialize()
      CA_SetApplicationID(3,4)
      C_OpenSession()
      C_GetSessionInfo()
      // Session info shows session
      // already logged in.
      <perform work, no login
      necessary>

C_Logout()

      C_GetSessionInfo()
      // Session info shows session
      // logged out.

C_CloseSession()
      C_CloseSession()
C_Finalize()
      C_Finalize()
```

The following code fragments show how one process might login for others:

Setup app:

```
C_Initialize()
CA_SetApplicationID(7,9)
CA_OpenApplicationID(slot,7,9)
C_OpenSession(slot)
C_Login()
C_CloseSession()
```

Spawn many child applications:

```
C_Finalize()
```

Terminate each child app:

```
      C_Initialize()
      CA_SetApplicationID(7,9)
      C_OpenSession(slot)
      <perform work, no login necessary>
```

Takedown app:

Terminate child applications:

```

        C_CloseSession()
        C_Finalize()
C_Initialize()
CA_CloseApplicationID(slot,7,9)
C_Finalize()

```

Named Curves and User-Defined Parameters

SafeNet Luna PCIe HSM is a PKCS#11-oriented device. The HSM firmware statically defines NIST named curve OIDs and curve parameters by default. You can also define other non-NIST curve OIDs and parameters such as Brainpool. SafeNet Luna PCIe HSM can decode and use the `ecParameters` structure for key generation, signing, and verification.

Curve Validation Limitations

The HSM can validate the curve parameters, but domain parameter validation guarantees only the consistency/sanity of the parameters and the most basic, well-known security properties. The HSM has no way of judging the quality of a user-specified curve.

It is therefore important that you perform Known Answer Tests to verify the operation of the HSM for any new Domain Parameter.set. To maintain NIST-FIPS compatibility the feature is selectively enabled with the feature being disabled by default. Therefore the Administrator must 'opt-in' by actively choosing to enable the appropriate HSM policy. Among other effects, this causes the HSM to display a shell/console message to the effect that the HSM is not operating in FIPS mode.

Storing Domain Parameters

Under PKCS#11 v2.20, Domain Parameters are stored in object attribute `CKA_EC_PARAMS`. The value of this parameter is the DER encoding of an ANSI X9.62 Parameters value.

```

Parameters ::= CHOICE {
ecParameters ECParameters,
namedCurve CURVES.&id({CurveNames}),
implicitlyCA NULL
}

```

Because PKCS#11 states that the `implicitlyCA` is not supported by cryptoki, therefore the `CKA_EC_PARAMS` attribute must contain the encoding of an `ecParameters` or a `namedCurve`. Cryptoki holds ECC key pairs in separate Private and Public key objects. Each object has its own `CKA_EC_PARAMS` attribute which must be provided when the object is created and cannot be subsequently changed.

Cryptoki also supports `CKO_DOMAIN_PARAMETERS` objects. These store Domain Parameters but perform no cryptographic operations. A Domain Parameters object is really only for storage. To generate a key pair, you must extract the attributes from the Domain Parameters object and insert them in the `CKA_EC_PARAMS` attribute of the Public key template. Cryptoki can create new ECC Public and Private key objects and Domain Parameters objects in the following ways:

- > Objects can be directly stored using the `C_CreateObject` command.
- > Public and private key objects can be generated internally with the `C_GenerateKeyPair` command and the `CKM_EC_KEY_PAIR_GEN` mechanism.

- Objects can be imported in encrypted form using C_UnwrapKey command.

Using Domain Parameters

ECC keys may be used for Signature Generation and Verification with the CKM_ECDSA and CKM_ECDSA_SHA1 mechanism and Encryption and Decryption with the CKM_ECIES mechanism. These three mechanism are enhanced so that they fetch the Domain Parameters from the CKA_EC_PARAMS attribute for both ecParameters and namedCurve choice and not just namedCurve choice.

User Friendly Encoder

Using ECC with Cryptoki to create or generate ECC keys requires that the CKA_EC_PARAMS attribute be specified. This is a DER encoded binary array. Usually in public documents describing ECC curves the Domain Parameters are specified as a series of printable strings so the programmer faces the problem of converting these to the correct format for Cryptoki use.

The cryptoki library is extended to support functions called CA_EncodeECPrimeParams and CA_EncodeECChar2Params which allow an application to specify the parameter details of a new curve. These functions implement DER encoders to build the CKA_EC_PARAMS attribute from large integer presentations of the Domain Parameter values.

Refer to "[Sample Domain Parameter Files](#)" on page 321.

Application Interfaces

CA_EncodeECPrimeParams

```
#include "cryptoki.h"
```

```
CK_RV CA_ EncodeECPrimeParams (
    CK_BYTE_PTR DerECPParams,CK_ULONG_PTR DerECPParams Len
    CK_BYTE_PTR prime,CK_USHORT primelen,
    CK_BYTE_PTR a,CK_USHORT alen,
    CK_BYTE_PTR b,CK_USHORT blen,
    CK_BYTE_PTR seed,CK_USHORT seedlen,
    CK_BYTE_PTR x,CK_USHORT xlen,
    CK_BYTE_PTR y,CK_USHORT ylen,
    CK_BYTE_PTR order,CK_USHORT orderlen,
    CK_BYTE_PTR cofactor,CK_USHORT cofactorlen,
);
```

Do DER enc of ECC Domain Parameters Prime

Parameters

DerECPParams	Resultant Encoding (length prediction supported if NULL).
DerECPParamsLen	Buffer len/Length of resultant encoding
prime	Prime modulus

primelen	Prime modulus len
a	Elliptic Curve coefficient a
alen	Elliptic Curve coefficient a length
b	Elliptic Curve coefficient b
blen	Elliptic Curve coefficient b length
seed	Seed (optional may be NULL)
seedlen	Seed length
x	Elliptic Curve point X coord
xlen	Elliptic Curve point X coord length
y	Elliptic Curve point Y coord
ylen	Elliptic Curve point Y coord length
order	Order n of the Base Point
orderlen	Order n of the Base Point length
cofactor	The integer $h = \#E(F_q)/n$ (optional)
cofactorlen	h length
Return	Status of operation. CKR_OK if ok.

CA_EncodeECChar2Params

```
#include "cryptoki.h"
```

```
CK_RV CA_EncodeECChar2Params (
    CK_BYTE_PTR DerECPParams,    CK_ULONG_PTR DerECPParams Len
    CK_USHORT m,
    CK_USHORT k1,
    CK_USHORT k2,
    CK_USHORT k3,
    CK_BYTE_PTR a,CK_USHORT alen,
    CK_BYTE_PTR b,CK_USHORT blen,
    CK_BYTE_PTR seed,CK_USHORT seedlen,
    CK_BYTE_PTR x,CK_USHORT xlen,
    CK_BYTE_PTR y,CK_USHORT ylen,
    CK_BYTE_PTR order,CK_USHORT orderlen,
    CK_BYTE_PTR cofactor,CK_USHORT cofactorlen,
);
```

Do DER enc of ECC Domain Parameters 2^M

Parameters

DerECPParams	Resultant Encoding (length prediction supported if NULL).
DerECPParamsLen	Buffer len/Length of resultant encoding
M	Degree of field
k1	parameter in trinomial or pentanomial basis polynomial
k2	parameter in pentanomial basis polynomial
k3	parameter in pentanomial basis polynomial
a	Elliptic Curve coefficient a
alen	Elliptic Curve coefficient a length
b	Elliptic Curve coefficient b
blen	Elliptic Curve coefficient b length
seed	Seed (optional may be NULL)
seedlen	Seed length
x	Elliptic Curve point X coord
xlen	Elliptic Curve point X coord length
y	Elliptic Curve point Y coord
ylen	Elliptic Curve point Y coord length
order	Order n of the Base Point
orderlen	Order n of the Base Point length
cofactor	The integer $h = \#E(F_q)/n$ (optional)
cofactorlen	h length
Return	Status of operation. CKR_OK if ok.

Sample Domain Parameter Files

The following examples show some sample domain parameter files.

brainpoolP512r1

```

#
#This file describes the domain parameters of an EC curve
#
#File contains lines of text. All lines not of the form key=value are ignored.
#All values must be Hexidecimal numbers except m, k, k1, k2 and k3 which are decimal.
#Lines starting with '#' are comments.
#
#Keys recognised for fieldID values are -
#p          - only if the Curve is based on a prime field
#m          - only if the curve is based on a 2^M field
#k1, k2, k3 - these three only if 2^M field
#
#You should have these combinations of fieldID values -
#p          - if Curve is based on a prime field
#m,k1,k2,k3 - if curve is based on 2^M
#
#These are the values common to prime fields and polynomial fields.
#a          - field element A
#b          - field element B
#s          - this one is optional
#x          - field element Xg of the point G
#y          - field element Yg of the point G
#q          - order n of the point G
#h          - (optional) cofactor h
#
#
# Curve name brainpoolP512r1

p=AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E
62881FF2F2D82C68528AA6056583A48F3

a=7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B
57F1117A72BF2C7B9E7C1AC4D77FC94CA

b=3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E6
7984050B75EBAE5DD2809BD638016F723

x=81AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5
7FC6D5047406A5E688B352209BCB9F822

y=7DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763A
ED1CA2B2FA8F0540678CD1E0F3AD80892

q=AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC104
71DB1D381085DDADDB58796829CA90069
h          = 1

```

Bad Parameter File

```

#
#This file describes the domain parameters of an EC curve
#
#File contains lines of text. All lines not of the form key=value are ignored.
#All values must be Hexidecimal numbers except m, k, k1, k2 and k3 which are decimal
#Lines starting with '#' are comments.
#

```


Curve Name(s)	OID (dot)	OID (byte)
brainpoolP320r1	1.3.36.3.3.2.8.1.1.9	06 09 2B 24 03 03 02 08 01 01 09
brainpoolP320t1	1.3.36.3.3.2.8.1.1.10	06 09 2B 24 03 03 02 08 01 01 0a
brainpoolP384r1	1.3.36.3.3.2.8.1.1.11	06 09 2B 24 03 03 02 08 01 01 0b
brainpoolP384t1	1.3.36.3.3.2.8.1.1.12	06 09 2B 24 03 03 02 08 01 01 0c
brainpoolP512r1	1.3.36.3.3.2.8.1.1.13	06 09 2B 24 03 03 02 08 01 01 0d
brainpoolP512t1	1.3.36.3.3.2.8.1.1.14	06 09 2B 24 03 03 02 08 01 01 0e
c2pnb163v1 (X9.62 c2pnb163v1)	1.2.840.10045.3.0.1	06 08 2A 86 48 CE 3D 03 00 01
c2pnb163v2 (X9.62 c2pnb163v2)	1.2.840.10045.3.0.2	06 08 2A 86 48 CE 3D 03 00 02
c2pnb163v3 (X9.62 c2pnb163v3)	1.2.840.10045.3.0.3	06 08 2A 86 48 CE 3D 03 00 03
c2pnb176w1 (X9.62 c2pnb176w1) c2pnb176v1 (X9.62 c2pnb176v1)	1.2.840.10045.3.0.4	06 08 2A 86 48 CE 3D 03 00 04
c2pnb208w1 (X9.62 c2pnb208w1)	1.2.840.10045.3.0.10	06 08 2A 86 48 CE 3D 03 00 0A
c2pnb272w1 (X9.62 c2pnb272w1)	1.2.840.10045.3.0.16	06 08 2A 86 48 CE 3D 03 00 10
c2pnb304w1 (X9.62 c2pnb304w1)	1.2.840.10045.3.0.17	06 08 2A 86 48 CE 3D 03 00 11
c2pnb368w1 (X9.62 c2pnb368w1)	1.2.840.10045.3.0.19	06 08 2A 86 48 CE 3D 03 00 13
c2tnb191v1 (X9.62 c2tnb191v1)	1.2.840.10045.3.0.5	06 08 2A 86 48 CE 3D 03 00 05
c2tnb191v2 (X9.62 c2tnb191v2)	1.2.840.10045.3.0.6	06 08 2A 86 48 CE 3D 03 00 06
c2tnb191v3 (X9.62 c2tnb191v3)	1.2.840.10045.3.0.7	06 08 2A 86 48 CE 3D 03 00 07
c2tnb239v1 (X9.62 c2tnb239v1)	1.2.840.10045.3.0.11	06 08 2A 86 48 CE 3D 03 00 0B
c2tnb239v2 (X9.62 c2tnb239v2)	1.2.840.10045.3.0.12	06 08 2A 86 48 CE 3D 03 00 0C
c2tnb239v3 (X9.62 c2tnb239v3)	1.2.840.10045.3.0.13	06 08 2A 86 48 CE 3D 03 00 0D
c2tnb359v1 (X9.62 c2tnb359v1)	1.2.840.10045.3.0.18	06 08 2A 86 48 CE 3D 03 00 12
c2tnb431r1 (X9.62 c2tnb431r1)	1.2.840.10045.3.0.20	06 08 2A 86 48 CE 3D 03 00 14

Curve Name(s)	OID (dot)	OID (byte)
Ed25519 (edwards25519)	1.3.6.1.4.1.11591.15.1	06 09 2B 06 01 04 01 DA 47 0F 01
prime192v1 (X9.62 prime192v1, secp192r1)	1.2.840.10045.3.1.1	06 08 2A 86 48 CE 3D 03 01 01
prime192v2 (X9.62 prime192v2)	1.2.840.10045.3.1.2	06 08 2A 86 48 CE 3D 03 01 02
prime192v3 (X9.62 prime192v3)	1.2.840.10045.3.1.3	06 08 2A 86 48 CE 3D 03 01 03
prime239v1 (X9.62 prime239v1)	1.2.840.10045.3.1.4	06 08 2A 86 48 CE 3D 03 01 04
prime239v2 (X9.62 prime239v2)	1.2.840.10045.3.1.5	06 08 2A 86 48 CE 3D 03 01 05
prime239v3 (X9.62 prime239v3)	1.2.840.10045.3.1.6	06 08 2A 86 48 CE 3D 03 01 06
prime256v1 (X9.62 prime256v1, secp256r1)	1.2.840.10045.3.1.7	06 08 2A 86 48 CE 3D 03 01 07
secp112r1	1.3.132.0.6	06 05 2B 81 04 00 06
secp112r2	1.3.132.0.7	06 05 2B 81 04 00 07
secp128r1	1.3.132.0.28	06 05 2B 81 04 00 1C
secp128r2	1.3.132.0.29	06 05 2B 81 04 00 1D
secp160k1	1.3.132.0.9	06 05 2B 81 04 00 09
secp160r1	1.3.132.0.8	06 05 2B 81 04 00 08
secp160r2	1.3.132.0.30	06 05 2B 81 04 00 1E
secp192k1	1.3.132.0.31	06 05 2B 81 04 00 1F
secp224k1	1.3.132.0.32	06 05 2B 81 04 00 20
secp224r1	1.3.132.0.33	06 05 2B 81 04 00 21
secp256k1	1.3.132.0.10	06 05 2B 81 04 00 0A
secp384r1	1.3.132.0.34	06 05 2B 81 04 00 22
secp521r1	1.3.132.0.35	06 05 2B 81 04 00 23
sect113r1	1.3.132.0.4	06 05 2B 81 04 00 04
sect113r2	1.3.132.0.5	06 05 2B 81 04 00 05

Curve Name(s)	OID (dot)	OID (byte)
sect131r1	1.3.132.0.22	06 05 2B 81 04 00 16
sect131r2	1.3.132.0.23	06 05 2B 81 04 00 17
sect163k1	1.3.132.0.1	06 05 2B 81 04 00 01
sect163r1	1.3.132.0.2	06 05 2B 81 04 00 02
sect163r2	1.3.132.0.15	06 05 2B 81 04 00 0F
sect193r1	1.3.132.0.24	06 05 2B 81 04 00 18
sect193r2	1.3.132.0.25	06 05 2B 81 04 00 19
sect233k1	1.3.132.0.26	06 05 2B 81 04 00 1A
sect233r1	1.3.132.0.27	06 05 2B 81 04 00 1B
sect239k1	1.3.132.0.3	06 05 2B 81 04 00 03
sect283k1	1.3.132.0.16	06 05 2B 81 04 00 10
sect283r1	1.3.132.0.17	06 05 2B 81 04 00 11
sect409k1	1.3.132.0.36	06 05 2B 81 04 00 24
sect409r1	1.3.132.0.37	06 05 2B 81 04 00 25
sect571k1	1.3.132.0.38	06 05 2B 81 04 00 26
sect571r1	1.3.132.0.39	06 05 2B 81 04 00 27
X25519 (curve25519)	1.3.6.1.4.1.3029.1.5.1	06 0a 2b 06 01 04 01 97 55 01 05 01

For additional information about the Elliptic Curve specification, refer to this article:

<http://www.ietf.org/rfc/rfc4492.txt>

Capability and Policy Configuration Control Using the SafeNet API

The configuration and control of the SafeNet Luna PCIe HSM is provided by a set of capabilities and policies which you can query and set using the SafeNet API. See for more information.

HSM Capabilities and Policies

Each HSM has a set of capabilities. An HSM's capability set defines and controls the behavior of the HSM.

HSM behavior can be further modified through changing policies. The HSM Admin can refine the behavior of an HSM by changing the policy settings.

HSM Partition Capabilities and Policies

Each HSM can support one-or-more virtual HSMs called HSM Partitions (may also be called “containers” in some areas of the API), which are used by properly authenticated remote clients to perform cryptographic operations.

Each HSM Partition has a set of capabilities. An HSM Partition's capability set defines and controls the behavior of the HSM partition.

HSM Partition behavior can be further modified through changing policies. The HSM Admin can refine the behavior of an HSM Partition by changing the policy settings. Different partitions can have different values for the configuration elements which apply to specific HSM Partitions – in other words, if a policy is set to a given value for one HSM Partition, the policy can be set to a different value for another HSM Partition on the same HSM.

In some cases, a partition policy change is destructive.

Policy Refinement

For every policy set element, there is a corresponding capability set element (the reverse is not true – there can be some capability set elements that do not have corresponding policy set elements). The value of a policy set element can be modified by the HSM Admin, but only within the limitations imposed by the corresponding capability set element.

For example, there is a policy set element which determines how many failed login attempts may be made before a Partition is deleted or locked out. There is also a corresponding capability set element for the same purpose. The policy element may be modified by the HSM Admin, but may only be set to a value less than or equal to that of the capability set element. So if the capability set element has a value of 10, the HSM Admin can set the policy to a value less than or equal to 10.

In general, the HSM Admin may modify policy set elements to make the HSM or partition policy more restrictive than that imposed by the capability set elements. The HSM Admin can not make the HSM or HSM Partition policy less restrictive or enable functionality that is disabled through capability settings.

Policy Types

There are three types of policy elements, as follows:

Normal policy elements	May be set at any time by the HSM Admin. The values which may be set are limited only by the corresponding capability element as described in the previous section (i.e. the policy element can be set only to a value less than or equal to the capability set element).
Destructive policy elements	May be set at any time, but setting them results in the erasure of any partitions and their contents. Policy elements are destructive if changing them significantly affects the security policy of the HSM.

Write-restricted policy elements

Cannot be modified directly, but instead are affected by other actions that can be taken.

Querying and Modifying HSM Configuration

The following are the relevant functions (found in **sfnt_extensions.h**):

- > CK_RV CK_ENTRY CA_GetConfigurationElementDescription(
- > CK_SLOT_ID slotID,
- > CK_ULONG ullsContainerElement,
- > CK_ULONG ullsCapabilityElement,
- > CK_ULONG ulElementId,
- > CK_ULONG_PTR pulElementBitLength,
- > CK_ULONG_PTR pulElementDestructive,
- > CK_ULONG_PTR pulElementWriteRestricted,
- > CK_CHAR_PTR pDescription);
- > CK_RV CK_ENTRY CA_GetHSMCapabilitySet(
- > CK_SLOT_ID uPhysicalSlot,
- > CK_ULONG_PTR pulCapIdArray,
- > CK_ULONG_PTR pulCapIdSize,
- > CK_ULONG_PTR pulCapValArray,
- > CK_ULONG_PTR pulCapValSize);
- > CK_RV CK_ENTRY CA_GetHSMCapabilitySetting (
- > CK_SLOT_ID slotID,
- > CK_ULONG ulPolicyId,
- > CK_ULONG_PTR pulPolicyValue);
- > CK_RV CK_ENTRY CA_GetHSMPolicySet(
- > CK_SLOT_ID uPhysicalSlot,
- > CK_ULONG_PTR pulPolicyIdArray,
- > CK_ULONG_PTR pulPolicyIdSize,
- > CK_ULONG_PTR pulPolicyValArray,
- > CK_ULONG_PTR pulPolicyValSize);
- > CK_RV CK_ENTRY CA_GetHSMPolicySetting (
- > CK_SLOT_ID slotID,
- > CK_ULONG ulPolicyId,

```

> CK_ULONG_PTR pulPolicyValue);
> CK_RV CK_ENTRY CA_GetContainerCapabilitySet(
> CK_SLOT_ID uPhysicalSlot,
> CK_ULONG ulContainerNumber,
> CK_ULONG_PTR pulCapIdArray,
> CK_ULONG_PTR pulCapIdSize,
> CK_ULONG_PTR pulCapValArray,
> CK_ULONG_PTR pulCapValSize );
> CK_RV CK_ENTRY CA_GetContainerCapabilitySetting (
> CK_SLOT_ID slotID,
> CK_ULONG ulContainerNumber,
> CK_ULONG ulPolicyId,
> CK_ULONG_PTR pulPolicyValue);
> CK_RV CK_ENTRY CA_GetContainerPolicySet(
> CK_SLOT_ID uPhysicalSlot,
> CK_ULONG ulContainerNumber,
> CK_ULONG_PTR pulPolicyIdArray,
> CK_ULONG_PTR pulPolicyIdSize,
> CK_ULONG_PTR pulPolicyValArray,
> CK_ULONG_PTR pulPolicyValSize );
> CK_RV CK_ENTRY CA_GetContainerPolicySetting(
> CK_SLOT_ID uPhysicalSlot,
> CK_ULONG ulContainerNumber,
> CK_ULONG ulPolicyId,
> CK_ULONG_PTR pulPolicyValue);
> CK_RV CK_ENTRY CA_SetHSMPolicy (
> CK_SESSION_HANDLE hSession,
> CK_ULONG ulPolicyId,
> CK_ULONG ulPolicyValue);
> CK_RV CK_ENTRY CA_SetDestructiveHSMPolicy (
> CK_SESSION_HANDLE hSession,
> CK_ULONG ulPolicyId,
> CK_ULONG ulPolicyValue);
> CK_RV CK_ENTRY CA_SetContainerPolicy (
> CK_SESSION_HANDLE hSession,

```

- > CK_ULONG ulContainer,
- > CK_ULONG ulPolicyId,
- > CK_ULONG ulPolicyValue);

The **CA_GetConfigurationElementDescription()** Function

The **CA_GetConfigurationElementDescription()** function requires that you pass in a zero or one value to indicate whether the element you are querying is an HSM Partition (container) element or an HSM element, and another zero/one value to define whether it is a capability or policy that you are interested in. You also pass in the id of the element and a character buffer of at least 60 characters. The function then returns the size of the element value (in bits), an indication of whether the element is destructive, an indication of whether the policy (if it is a policy) is write-restricted, and it also writes the description string into the buffer that you provided.

The **CA_Get{HSM|Container}{Capability|Policy}Set()** Functions

The various **CA_Get{HSM|Container}{Capability|Policy}Set()** functions all return (in the word arrays provided) a complete list of element id/value pairs for the set specified. For example, **CA_GetHSMCapabilitySet()** returns a list of all HSM capability elements and their values. The parameters for these functions include a list pointer and length pointer for each of the element ids and element values. On calling the function, you should provide a buffer or a null pointer for each of the lists, and the length value should be initialized to the size of the buffer. On return, the buffer (if given) is populated, and the length is updated to the real length of the list. If the buffer is given but is not large enough, an error results.

Typically you would invoke the function twice: call the function the first time with null buffer pointers so that the real length necessary is returned, then allocate the necessary buffers and call the function a second time, giving the real buffers.

The various **CA_Get{HSM|Container}{Capability|Policy}Setting()** functions allow you to query a specific element value. Provide the element id and the function returns the value.

The **CA_Set...()** Functions

The various **CA_Set...()** functions allow you to set individual HSM and HSM Partition policies. There are two varieties for setting HSM policies, because changing the value of a destructive HSM policy results in the HSM being cleared of any Partitions and their contents. To make it clear when this is going to happen, the appropriate set function must be called based on whether the HSM policy is destructive or not (which you can determine with the **CA_GetConfigurationElementDescription()** function).

Connection Timeout

The connection timeout is not configurable.

Linux and Unix Connection Timeout

On Unix platforms, the client performs a **connect** on the socket. If the socket is busy or unavailable, the client performs a **select** on the socket with the timeout set to 10 seconds (hardcoded). If the **select** call returns before the timeout, then the client is able to connect. If not then it fails. This prevents the situation where some Unix operating systems can block for several minutes when SafeNet Luna PCIe HSM is unavailable.

Windows Connection Timeout

On Windows platforms, **connect** is called without **select**, relying upon the default Windows timeout of approximately 20 seconds.

CHAPTER 6: Design Considerations

This chapter provides guidance for creating applications that use specific SafeNet Luna PCIe HSM configurations or features. It contains the following topics:

- > ["PED-Authenticated HSMs" below](#)
- > ["High Availability \(HA\) Implementations" on page 336](#)
- > ["Key Attribute Defaults" on page 338](#)
- > ["Object Usage Count" on page 340](#)
- > ["Migrating Keys From Software to a SafeNet Luna PCIe HSM" on page 343](#)
- > ["Audit Logging" on page 367](#)

PED-Authenticated HSMs

In systems or applications using SafeNet Luna PCIe HSMs, Luna PED is required for FIPS 140-2 level 3 security. In normal use, Luna PED supplies PINs and certain other critical security parameters to the token/HSM, invisibly to the user. This prevents other persons from viewing PINs, etc. on a computer screen or watching them typed on a keyboard, which in turn prevents such persons from illicitly cloning token or HSM contents.

Two classes of users operate Luna PED: the ordinary HSM Partition Owner, and the HSM Administrator, (also called Security Officer or SO). The person handling new HSMs and using Luna PED is normally the HSM SO, who:

- > Initializes the HSM
- > Conducts HSM maintenance, such as firmware and capability upgrades
- > Initializes HSM Partitions and tokens
- > Creates users (sets PINs)
- > Changes policy settings
- > Changes passwords

Following these initial activities, the Luna PED may be required to present the HSM Partition Owner's PED key or keys (in case of MofN operations) to enable ordinary signing cryptographic operations carried out by your applications.

With the combination of Activation and AutoActivation, the black PED key is required only upon initial authentication and then not again unless the authentication is interrupted by power failure or by deliberate action on the part of the PED key holders.

About CKDemo with Luna PED

As its name suggests, CKDemo (CryptoKi Demonstration) is a demonstration program, allowing you to explore the capabilities and functions of several SafeNet products. The demo program breaks out a number of PKCS 11 functions, as well as the SafeNet extensions to Cryptoki that allow the enhanced capabilities of our HSMs. However the flexibility, combined with the bare-bones nature of the program, can result in some confusion as to whether certain operations and combinations are permissible. Where these come up, in the explanation of CKDemo with SafeNet Luna PCIe HSM with PED [Trusted Path] Authentication, and Luna PED, they are mentioned and explained if necessary.

The demo program appears to make it optional to permit several of the security operations via the keyboard and program interface, or to require that they be done only via the Luna PED keypad. In fact, the option is dictated by the SafeNet Luna PCIe HSM, as it was configured and shipped from the factory, and cannot be changed by you. That is, you can use CKDemo to work/experiment with either type of SafeNet Luna PCIe HSM (i.e., SafeNet Luna PCIe HSM with Password Authentication or SafeNet Luna PCIe HSM with PED Authentication, requiring Luna PED), but you cannot make one type behave like the other.

Security and design requirements, enforced by the SafeNet Luna PCIe HSM with PED Authentication HSM, dictate that use of Luna PED be mandatory within the applications that you develop for it.

Interchangeability

As mentioned above, several secrets and security parameters related to HSMs are imprinted on PED keys which provide "something you have" access control, as opposed to the "something you know" access control provided by password-authenticated HSMs. The HSM can create each type of secret, which is then also imprinted on a suitably labeled PED key. Alternatively, the secret can be accepted from a PED key (previously imprinted by another HSM) and imprinted on the current HSM. This is mandatory for the cloning domain, when HSMs (or HSM partitions) are to clone objects one to the other. It is optional for the other HSM secrets, as a matter of convenience or of your security policy, allowing more than one HSM to be accessed for administration by a single SO (blue PED key holder) or more than one HSM Partition to be administered by a single Partition Owner/User.

PED keys that have never been imprinted are completely interchangeable. They can be used with any modern SafeNet Luna PCIe HSM, and can be imprinted with any of the various secrets. The self-stick labels are provided as a visual identifier of which type of secret has been imprinted on a PED key, or is about to be imprinted. Imprinted PED keys are tied to their associated HSMs and cannot be used to access HSMs or partitions that have been imprinted with different secrets.

Any Luna PED2 can be used with any SafeNet Luna PCIe HSM - the PED itself contains no secrets; it simply provides the interface between you and your HSM(s). The exception is that only some Luna PEDs have the capability to be used remotely from the HSM. Any Remote-capable Luna PED2 is interchangeable with any other Remote-capable Luna PED2, and any Luna PED2 (remote-capable or not) is interchangeable with any other when locally connected to a SafeNet Luna PCIe HSM.

HSM Partitions and Backup Tokens and PED keys can be "re-cycled" for use in different combinations, but this reuse requires re-initializing the HSM(s) and re-imprinting the PED keys with new secrets or security parameters. Re-initializing a token or HSM wipes previous information from it. Re-imprinting a PED key overwrites any previous information it carried (PIN, domain, etc.).

Startup

Luna PED expects to be connected to a SafeNet Luna PCIe HSM with Trusted Path Authentication. At power-up, it presents a message showing its firmware version. After a few seconds, the message changes to "Awaiting command..." The Luna PED is waiting for a command from the token/HSM.

The Luna PED screen remains in this status until the CKDemo program, or your own application, initiates a command through the token/HSM.

For the purposes of demonstration, you would now go ahead and create some objects and perform other transactions with the HSM.

NOTE To perform most actions you must be logged in. CKDemo may not remind you before you perform actions out-of-order, but it generates error messages after such attempts. If you receive an error message from the program, review your recent actions to determine if you have logged out or closed sessions and then not formally logged into a new session before attempting to create an object or perform other token/HSM actions. When you do wish to end activities, be sure to formally log out and close sessions. An orderly shutdown of your application should include logging out any users and closing all sessions on HSMs.

Cloning of Tokens

To securely copy the contents of a SafeNet Luna PCIe HSM Partition to another SafeNet Luna PCIe HSM Partition (on the same SafeNet Luna PCIe HSM or on another), you must perform a backup to a SafeNet Luna Backup HSM from the source HSM Partition followed by a restore operation from the Backup HSM to the new destination HSM Partition. This is done via LunaSH command line, and cannot be accomplished via CKDemo.

High Availability (HA) Implementations

If you use the SafeNet Luna PCIe HSM HA feature then the calls to the SafeNet Luna PCIe HSMs are load-balanced. The session handle that the application receives when it opens a session is a virtual one and is managed by the HA code in the library. The actual sessions with the HSM are established by the HA code in the library and hidden from the application and will come and go as necessary to fulfill application level requests.

Before the introduction of HA AutoRecovery, bringing a failed/lost group member back into the group (recovery) was a manual procedure.

The Administration & Maintenance section contains a general description of the how the HA AutoRecovery function works, in practice.

For every PKCS#11 call, the HA recover logic will check to see if we need to perform auto recovery to a disconnected appliance. If there is a disconnected appliance then it will try to reconnect to that appliance before it proceeds with the current PKCS#11 call.

The HA recovery logic is designed in such a way that it will try to reconnect to an appliance only every X secs and N number of times where X is pre-set to one minute, and N is configurable via Lunacm.

For HA recovery attempts:

- > The default retry interval is 60 seconds.
- > The default number of retries is effectively infinite.

- The HA configuration section in the **Chrystoki.conf/crystoki.ini** file is created and populated when either the interval or the number of retries is specified in the LunaCM commands "[hagroup retry](#)" on page 1 and "[hagroup interval](#)" on page 1.

The following is the pseudo code of the HA logic

```

if (disconnected_member > 0 and recover_attempt_count < N and time_now - last_recover_attempt >
X) then
  performance auto recovery
  set last_recover_attempt equal to time_now
  if (recovery failed) then
    increment recover_attempt_count by 1
  else
    decrement disconnected_member by 1
    reset recover_attempt_count to 0
  end if
end if

```

The HA auto recovery design runs within a PKCS#11 call. The responsiveness of recovering a disconnected member is greatly influenced by the frequency of PKCS#11 calls from the user application. Although the logic shows that it will attempt to recover a disconnected client in X secs, in reality, it will not run until the user application makes the next PKCS#11 call.

Detecting the Failure of an HA Member

When an HA Group member first fails, the HA status for the group shows "device error" for the failed member. All subsequent calls return "token not present", until the member (HSM Partition or PKI token) is returned to service.

Here is an example of two such calls using CKDemo:

```

Enter your choice : 52
Slots available:
  slot#1 - LunaNet Slot
  slot#2 - LunaNet Slot
  slot#3 - HA Virtual Card Slot

Select a slot: 3

HA group 1599447001 status:
  HSM 599447001      - CKR_DEVICE_ERROR
  HSM 78665001      - CKR_OK
Status: Doing great, no errors (CKR_OK)

TOKEN FUNCTIONS
( 1) Open Session   ( 2) Close Session   ( 3) Login
( 4) Logout         ( 5) Change PIN      ( 6) Init Token
( 7) Init Pin       ( 8) Mechanism List  ( 9) Mechanism Info
(10) Get Info       (11) Slot Info       (12) Token Info
(13) Session Info  (14) Get Slot List  (15) Wait for Slot Event
(16) InitToken(ind) (17) InitPin (ind)  (18) Login (ind)
(19) CloneMofN

OBJECT MANAGEMENT FUNCTIONS
(20) Create object (21) Copy object    (22) Destroy object
(23) Object size  (24) Get attribute  (25) Set attribute
(26) Find object  (27) Display Object

SECURITY FUNCTIONS
(40) Encrypt file (41) Decrypt file  (42) Sign

```

(43) Verify (44) Hash file (45) Simple Generate Key
 (46) Digest Key

HIGH AVAILABILITY RECOVERY FUNCTIONS

(50) HA Init (51) HA Login (52) HA Status

KEY FUNCTIONS

(60) Wrap key (61) Unwrap key (62) Generate random number
 (63) Derive Key (64) PBE Key Gen (65) Create known keys
 (66) Seed RNG (67) EC User Defined Curves

CA FUNCTIONS

(70) Set Domain (71) Clone Key (72) Set MofN
 (73) Generate MofN (74) Activate MofN (75) Generate Token Keys
 (76) Get Token Cert (77) Sign Token Cert (78) Generate CertCo Cert
 (79) Modify MofN (86) Dup. MofN Keys (87) Deactivate MofN

CCM FUNCTIONS

(80) Module List (81) Module Info (82) Load Module
 (83) Load Enc Mod (84) Unload Module (85) Module function Call

OTHERS

(90) Self Test (94) Open Access (95) Close Access
 (97) Set App ID (98) Options

OFFBOARD KEY STORAGE:

(101) Extract Masked Object (102) Insert Masked Object
 (103) Multisign With Value (104) Clone Object
 (105) SIMExtract (106) SIMInsert
 (107) SimMultiSign

SCRIPT EXECUTION:

(108) Execute Script
 (109) Execute Asynchronous Script
 (110) Execute Single Part Script
 (0) Quit demo

Enter your choice : 52

Slots available:

slot#1 - LunaNet Slot
 slot#2 - LunaNet Slot
 slot#3 - HA Virtual Card Slot

Select a slot: 3

HA group 1599447001 status:

HSM 599447001 - CKR_TOKEN_NOT_PRESENT
 HSM 78665001 - CKR_OK

Status: Doing great, no errors (CKR_OK)

--- end ---

Key Attribute Defaults

The following default attribute settings are applied to generated keys/keypairs, and to unwrapped private/secret keys, unless your application specifies different values.

Management Attributes

Attribute	Default Value			
	Generated Public Keys	Generated Private Keys	Unwrapped Private/Secret Keys	Derived Secret Keys
CKA_TOKEN	0 (FALSE)	0 (FALSE)	0 (FALSE)	0 (FALSE)
CKA_PRIVATE	1 (TRUE) if Crypto Officer logged in 0 (FALSE) if Crypto Officer not logged in	1 (TRUE) if Crypto Officer logged in 0 (FALSE) if Crypto Officer not logged in	1 (TRUE) if Crypto Officer logged in 0 (FALSE) if Crypto Officer not logged in	1 (TRUE) if Crypto Officer logged in 0 (FALSE) if Crypto Officer not logged in
CKA_SENSITIVE	N/A	1 (TRUE)	1 (TRUE)	0 (FALSE)
CKA_MODIFIABLE	1 (TRUE)	1 (TRUE)	1 (TRUE)	1 (TRUE)
CKA_EXTRACTABLE	N/A	0 (FALSE)	0 (FALSE)	0 (FALSE)
CKA_ALWAYS_SENSITIVE	N/A	Always the same value as CKA_SENSITIVE	Always 0 (FALSE)	Inherited from base key(s) depending on CKA_SENSITIVE history*
CKA_NEVER_EXTRACTABLE	N/A	Always the opposite value of CKA_EXTRACTABLE	Always 0 (FALSE)	Inherited from base key(s) depending on CKA_EXTRACTABLE history**

* CKA_ALWAYS_SENSITIVE=1 assures that the key and the key(s) from which it was derived have always been sensitive (CKA_SENSITIVE=1). If a newly-derived key has CKA_ALWAYS_SENSITIVE=0, it means the key(s) from which it derives has had CKA_SENSITIVE=0 at some point.

** CKA_NEVER_EXTRACTABLE=1 assures that the key and the key(s) from which it was derived have never been extractable (CKA_EXTRACTABLE has always been set to 0). If a newly-derived key has CKA_NEVER_EXTRACTABLE=0, it means the key(s) from which it derives has had CKA_EXTRACTABLE=1 at some point.

Key Usage Attributes

Attribute	Default Value			
	Generated Public Keys	Generated Private Keys	Unwrapped Private/Secret Keys	Derived Secret Keys
CKA_ENCRYPT	0 (FALSE)	N/A	0 (FALSE)	0 (FALSE)
CKA_DECRYPT	N/A	0 (FALSE)	0 (FALSE)	0 (FALSE)
CKA_WRAP	0 (FALSE)	N/A	0 (FALSE)	0 (FALSE)
CKA_UNWRAP	N/A	0 (FALSE)	0 (FALSE)	0 (FALSE)
CKA_SIGN	N/A	0 (FALSE)	0 (FALSE)	0 (FALSE)
CKA_VERIFY	0 (FALSE)	N/A	0 (FALSE)	0 (FALSE)
CKA_DERIVE	0 (FALSE)	N/A	0 (FALSE)	0 (FALSE)

Vendor-defined key attributes

KEY ATTRIBUTE	DESCRIPTION
CKA_CCM_PRIVATE	Not used by the Luna HSM; it does not affect any of the HSM functionality. This is an old attribute that was used in the firmware 3.x HSMs, the Luna CA and Luna CA3 products.
CKA_OUID	This is a 12-byte unique identifier for the object, unique across all Luna HSMs. It can be used to identify the object across multiple HSM.
CKA_EKM_UID	This is not used by the Luna HSM, it does not affect any of the HSM functionality. It is intended to be used by our EKM Key Manager SHIM to store a KEY ID, so that the key manager can track keys efficiently. Customer applications should not use this (they should use the CKA_GENERIC_1/2/3 attributes defined below).
CKA_GENERIC_1/2/3	These are not used by the Luna HSM, and do not affect any of the HSM functionality. They are variable length attributes that store an array of CK_BYTE and are provided for customer applications to make use of, to store whatever data they want.

Object Usage Count

You may wish to create keys that have a limited number of uses. You can set attributes on a key object to track and limit the number of cryptographic operations that object may perform. The relevant attributes are:

- > CKA_USAGE_COUNT: the number of operations that have been performed using the key
- > CKA_USAGE_LIMIT: the maximum number of operations allowed for the key.

When the limit set by CKA_USAGE_LIMIT is reached, attempts to use the key for operations like encrypt/decrypt, sign/verify, etc. will return an error (CKR_KEY_NOT_ACTIVE).

Setting CKA_USAGE_LIMIT on a key using CKDEMO

You can use CKDEMO to set this limit for a specific key on the HSM.

To set CKA_USAGE_LIMIT on a key:

1. Navigate to the SafeNet Luna HSM Client directory and run CKDEMO.
2. Select **Option 1 (Open Session)**.
3. Select **Option 3 (Login)**, select the partition where the key is located, and present the Crypto Officer login credential.
4. If you do not know the key's object handle, select **Option 27 (Display Object)** and enter 0 to view a list of available objects.
5. Select **Option 25 (Set Attribute)** and enter the key's object handle when prompted.
6. Select **Sub-option 1 (Add Attribute)**, and **53 (CKA_USAGE_LIMIT)** from the list of attributes.
7. Enter the desired maximum number of uses in hexadecimal (Allowable range: 1 - FFFFFFFF).
8. Select **Option 27** and enter the key's object handle to view the key attributes. When you set CKA_USAGE_LIMIT in step 7, CKA_USAGE_COUNT is also set, with a value of 0:

```
Enter your choice: 27
```

```
Enter handle of object to display (0 to list available objects) : 247
Object handle=247
CKA_CLASS=0003 (3)
CKA_TOKEN=01
CKA_PRIVATE=01
CKA_LABEL=Generated RSA Private Key
CKA_KEY_TYPE=0000 (0)
CKA_SUBJECT=
CKA_ID=
CKA_SENSITIVE=01
CKA_DECRYPT=01
CKA_UNWRAP=01
CKA_SIGN=01
CKA_SIGN_RECOVER=00
CKA_DERIVE=00
CKA_START_DATE=
CKA_END_DATE=
CKA_MODULUS=bc613525ae8c5b30ca086c0e688f2f0ed6928805bf007d4fc...
CKA_MODULUS_BITS=0400 (1024)
CKA_PUBLIC_EXPONENT=010001
CKA_LOCAL=01
CKA_MODIFIABLE=01
CKA_EXTRACTABLE=01
CKA_ALWAYS_SENSITIVE=01
CKA_NEVER_EXTRACTABLE=00
CKA_CCM_PRIVATE=00
```

```

CKA_FINGERPRINT_SHA1=6beddef34f9f5c8023e3422daecd6bd91c2dc40d
CKA_OUID=b00800000300000d1b030100
CKA_X9_31_GENERATED=00
CKA_EKM_UID=
CKA_USAGE_LIMIT=000e (15)
CKA_USAGE_COUNT=0000 (0)
CKA_GENERIC_1=
CKA_GENERIC_2=
CKA_GENERIC_3=
CKA_FINGERPRINT_SHA256=a8293ea9ddb578bcc644279c9753de4df772958563d259bed28c5d2a2e04e7d

```

Status: Doing great, no errors (CKR_OK)

Using this key to perform cryptographic operations will now increment the value of CKA_USAGE_COUNT.

Creating multiple keys with CKA_USAGE_LIMIT using CKDEMO

If you are creating multiple, usage-limited keys in CKDEMO, you can simplify this procedure by changing a CKDEMO setting. You will then have the option to set a usage limit for all new keys created in that session.

To create multiple keys with CKA_USAGE_LIMIT set:

1. Navigate to the SafeNet Luna HSM Client directory and run CKDEMO.
2. Select **Option 98 (Options)**.
3. Select **Option 10 (Object Usage Counters)**.

Note that the option value has changed from "disabled" to "selectable".

4. Enter **0** to exit the (**Options**) menu.
5. Open a session and begin creating your new keys. In addition to setting the attributes governing key capabilities, you will be prompted to enter a value for CKA_USAGE_LIMIT (in hexadecimal):

```

Select type of key to generate
[ 1] DES      [ 2] DES2    [ 3] DES3      [ 5]  CAST3
[ 6] Generic [ 7] RSA      [ 8] DSA      [ 9]  DH      [10]  CAST5
[11] RC2     [12] RC4     [13] RC5     [14]  SSL3   [15]  ECDSA
[16] AES     [17] SEED    [18] KCDSA-1024 [19] KCDSA-2048
[20] DSA Domain Param [21] KCDSA Domain Param
[22] RSA X9.31 [23] DH X9.42 [24]  ARIA
[25] DH PKCS Domain Param [26] RSA 186-3 Aux Primes
[27] RSA 186-3 Primes [28] DH X9.42 Domain Param
[29] ECDSA with Extra Bits [30] EC Edwards
[31] EC Montgomery
> 7

```

Enter Key Length in bits: 1024

Enter Is Token Attribute [0-1]: 1

Enter Is Sensitive Attribute [0-1]: 1

Enter Is Private Attribute [0-1]: 1

Enter Is Modifiable Attribute [0-1]: 1

Enter Extractable Attribute [0-1]: 1

```

Enter Encrypt/Decrypt Attribute [0-1]: 1

Enter Sign/Verify Attribute [0-1]: 1

Enter Wrap/Unwrap Attribute [0-1]: 1

Enter Derive Attribute [0-1]: 1
Would you like to specify a usage count limit? [0-no, 1-yes]: 1
Please enter the limit in HEX: 0E
Generated RSA Public Key:      160 (0x000000a0)
Generated RSA Private Key:    247 (0x000000f7)

Status: Doing great, no errors (CKR_OK)

```

Migrating Keys From Software to a SafeNet Luna PCIe HSM

SafeNet Luna PCIe HSMs expect key material to be in PKCS#8 format. PKCS#8 format follows BER (Basic encoding rules)/DER (distinguished encoding rules) encoding. An example of this format can be found in the document "Some examples of PKCS standards" produced by RSA, and available on their web site (<http://www.rsasecurity.com/rsalabs/pkcs/index.html> at the bottom of the page, under "Related Documents").

Here is an example of a formatted key:

```

0x30,
0x82, 0x04, 0xbc, 0x02, 0x01, 0x00, 0x30, 0x0d, 0x06, 0x09, 0x2a, 0x86,
0x48, 0x86, 0xf7, 0x0d, 0x01, 0x01, 0x01, 0x05, 0x00, 0x04, 0x82, 0x04,
0xa6, 0x30, 0x82, 0x04, 0xa2, 0x02, 0x01, 0x00, 0x02, 0x82, 0x01, 0x01,
0x00, 0xb8, 0xb5, 0x0f, 0x49, 0x46, 0xb5, 0x5d, 0x58, 0x04, 0x8e, 0x52,
0x59, 0x39, 0xdf, 0xd6, 0x29, 0x45, 0x6b, 0x6c, 0x96, 0xbb, 0xab, 0xa5,
0x6f, 0x72, 0x1b, 0x16, 0x96, 0x74, 0xd5, 0xf9, 0xb4, 0x41, 0xa3, 0x7c,
0xe1, 0x94, 0x73, 0x4b, 0xa7, 0x23, 0xff, 0x61, 0xeb, 0xce, 0x5a, 0xe7,
0x7f, 0xe3, 0x74, 0xe8, 0x52, 0x5b, 0xd6, 0x5d, 0x5c, 0xdc, 0x98, 0x49,
0xfe, 0x51, 0xc2, 0x7e, 0x8f, 0x3b, 0x37, 0x5c, 0xb3, 0x11, 0xed, 0x85,
0x91, 0x15, 0x92, 0x24, 0xd8, 0xf1, 0x7b, 0x3d, 0x2f, 0x8b, 0xcd, 0x1b,
0x30, 0x14, 0xa3, 0x6b, 0x1b, 0x4d, 0x27, 0xff, 0x6a, 0x58, 0x84, 0x9e,
0x79, 0x94, 0xca, 0x78, 0x64, 0x01, 0x33, 0xc3, 0x58, 0xfc, 0xd3, 0x83,
0xeb, 0x2f, 0xab, 0x6f, 0x85, 0x5a, 0x38, 0x41, 0x3d, 0x73, 0x20, 0x1b,
0x82, 0xbc, 0x7e, 0x76, 0xde, 0x5c, 0xfe, 0x42, 0xd6, 0x7b, 0x86, 0x4f,
0x79, 0x78, 0x29, 0x82, 0x87, 0xa6, 0x24, 0x43, 0x39, 0x74, 0xfe, 0xf2,
0x0c, 0x08, 0xbe, 0xfa, 0x1e, 0x0a, 0x48, 0x6f, 0x14, 0x86, 0xc5, 0xcd,
0x9a, 0x98, 0x09, 0x2d, 0xf3, 0xf3, 0x5a, 0x7a, 0xa4, 0xe6, 0x8a, 0x2e,
0x49, 0x8a, 0xde,
0x73, 0xe9, 0x37, 0xa0, 0x5b, 0xef, 0xd0, 0xe0, 0x13, 0xac, 0x88, 0x5f,
0x59, 0x47, 0x96, 0x7f, 0x78, 0x18, 0x0e, 0x44, 0x6a, 0x5d, 0xec,
0x6e, 0xed, 0x4f, 0xf6, 0x6a, 0x7a, 0x58, 0x6b, 0xfe, 0x6c, 0x5a, 0xb9,
0xd2, 0x22, 0x3a, 0x1f, 0xdf, 0xc3, 0x09, 0x3f, 0x6b, 0x2e, 0xf1, 0x6d,
0xc3, 0xfb, 0x4e, 0xd4, 0xf2, 0xa3, 0x94, 0x13, 0xb0, 0xbf, 0x1e, 0x06,
0x2e, 0x29, 0x55, 0x00, 0xaa, 0x98, 0xd9, 0xe8, 0x77, 0x84, 0x8b, 0x3f,
0x5f, 0x5e, 0xf7, 0xf8, 0xa7, 0xe6, 0x02, 0xd2, 0x18, 0xb0, 0x52, 0xd0,
0x37, 0x2e, 0x53, 0x02, 0x03, 0x01, 0x00, 0x01, 0x02, 0x82, 0x01, 0x00,
0x0c, 0xdf, 0xd1, 0xe8, 0xf1, 0x9c, 0xc2, 0x9c, 0xd7, 0xf4, 0x73, 0x98,
0xf4, 0x87, 0xbd, 0x8d, 0xb2, 0xe1, 0x01, 0xf8, 0x9f, 0xac, 0x1f, 0x23,
0xdd, 0x78, 0x35, 0xe2, 0xd6, 0xd1, 0xf3, 0x4d, 0xb5, 0x25, 0x88, 0x16,
0xd1, 0x1a, 0x18, 0x33, 0xd6, 0x36, 0x7e, 0xc4, 0xc8, 0xe5, 0x5d, 0x2d,
0x74, 0xd5, 0x39, 0x3c, 0x44, 0x5a, 0x74, 0xb7, 0x7c, 0x48, 0xc1, 0x1f,
0x90, 0xe3, 0x55, 0x9e, 0xf6, 0x29, 0xad, 0xb4, 0x6d, 0x93, 0x78, 0xb3,

```

```

0xdc, 0x25, 0x0b, 0x9c, 0x73, 0x78, 0x7b, 0x93, 0x4c, 0xd3, 0x47, 0x09,
0xda, 0xe6, 0x69, 0x18, 0xc6, 0x0f, 0xfb, 0xa5, 0x95, 0xf5, 0xe8, 0x75,
0xe1, 0x01, 0x1b, 0xd3, 0x1c, 0xa2, 0x57, 0x03, 0x64, 0xdb, 0xf9, 0x5d,
0xf3, 0x3c, 0xa7, 0xd1, 0x4b, 0xb0, 0x90, 0x1b, 0x90, 0x62, 0xb4, 0x88,
0x30, 0x4b, 0x40, 0x4d, 0xcf, 0x7d, 0x89, 0x7a, 0xfb, 0x29, 0xc9, 0x64,
0x34, 0x0a, 0x52, 0xf6, 0x70, 0x7c, 0x76, 0x5a, 0x2e, 0x8f, 0x50, 0xd4,
0x92, 0x15, 0x97, 0xed, 0x4c, 0x2e, 0xf2, 0x3a, 0xd0, 0x58, 0x7e, 0xdb,
0xf1, 0xf4, 0xdd, 0x07, 0x76, 0x04, 0xf0, 0x55, 0x8b, 0x72, 0x2b, 0xa7,
0xa8, 0x78, 0x78, 0x67, 0xe6, 0xd8, 0xa5, 0xde, 0xe7, 0xc9, 0x1f, 0x5a,
0xa0, 0x89, 0xc7, 0x24, 0xa2, 0x71, 0xb6, 0x7b, 0x3b, 0xe6, 0x92, 0x69,
0x22, 0xaa, 0xe2, 0x47, 0x4b, 0x80, 0x3f, 0x6a, 0xab, 0xce, 0x4e, 0xcd,
0xe8, 0x94, 0x6c, 0xf7, 0x84, 0x73, 0x85, 0xfd, 0x85, 0x1d, 0xae, 0x81,
0xf7, 0xec, 0x12, 0x31, 0x7d, 0xc1, 0x99, 0xc0, 0x3c, 0x51, 0xb0, 0xdc,
0xb0, 0xba, 0x9c, 0x84, 0xb8, 0x70, 0xc2, 0x09, 0x7f, 0x96, 0x3d, 0xa1,
0xe2, 0x64, 0x27, 0x7a, 0x22, 0xb8, 0x75, 0xb9, 0xd1, 0x5f, 0xa5, 0x23,
0xf9, 0x62, 0xe0, 0x41, 0x02, 0x81, 0x81, 0x00, 0xf4, 0xf3, 0x08, 0xcf,
0x83, 0xb0, 0xab, 0xf2, 0x0f, 0x1a, 0x08, 0xaf, 0xc2, 0x42, 0x29, 0xa7,
0x9c, 0x5e, 0x52, 0x19, 0x69, 0x8d, 0x5b, 0x52, 0x29, 0x9c, 0x06, 0x6a,
0x5a, 0x32, 0x8f, 0x08, 0x45, 0x6c, 0x43, 0xb5, 0xac, 0xc3, 0xbb, 0x90,
0x7b, 0xec, 0xbb, 0x5d, 0x71, 0x25, 0x82, 0xf8, 0x40, 0xbf, 0x38, 0x00,
0x20, 0xf3, 0x8a, 0x38, 0x43, 0xde, 0x04, 0x41, 0x19, 0x5f, 0xeb, 0xb0,
0x50, 0x59, 0x10, 0xe1, 0x54, 0x62, 0x5c, 0x93, 0xd9, 0xdc, 0x63, 0x24,
0xd0, 0x17, 0x00, 0xc0, 0x44, 0x3e, 0xfc, 0xd1, 0xda, 0x4b, 0x24, 0xf7,
0xcb, 0x16, 0x35, 0xe6, 0x9f, 0x67, 0x96, 0x5f, 0xb0, 0x94, 0xde, 0xfa,
0xa1, 0xfd, 0x8c, 0x8a, 0xd1, 0x5c, 0x02, 0x8d, 0xe0, 0xa0, 0xa0, 0x02,
0x1d, 0x56, 0xaf, 0x13, 0x3a, 0x65, 0x5e, 0x8e, 0xde, 0xd1, 0xa8, 0x28,
0x8b, 0x71, 0xc9, 0x65, 0x02, 0x81, 0x81, 0x00, 0xc1, 0x0a, 0x47,
0x39, 0x91, 0x06, 0x1e, 0xb9, 0x43, 0x7c, 0x9e, 0x97, 0xc5, 0x09, 0x08,
0xbc, 0x22, 0x47, 0xe2, 0x96, 0x8e, 0x1c, 0x74, 0x80, 0x50, 0x6c, 0x9f,
0xef, 0x2f, 0xe5, 0x06, 0x3e, 0x73, 0x66, 0x76, 0x02, 0xbd, 0x9a, 0x1c,
0xfc, 0xf9, 0x6a, 0xb8, 0xf9, 0x36, 0x15, 0xb5, 0x20, 0x0b, 0x6b, 0x54,
0x83, 0x9c, 0x86, 0xba, 0x13, 0xb7, 0x99, 0x54, 0xa0, 0x93, 0x0d, 0xd6,
0x1e, 0xc1, 0x12, 0x72, 0x0d, 0xea, 0xb0, 0x14, 0x30, 0x70, 0x73, 0xef,
0x6b, 0x4c, 0xae, 0xb6, 0xff, 0xd4, 0xbb, 0x89, 0xa1, 0xec, 0xca, 0xa6,
0xe9, 0x95, 0x56, 0xac, 0xe2, 0x9b, 0x97, 0x2f, 0x2c, 0xdf, 0xa3, 0x6e,
0x59, 0xff, 0xcd, 0x3c, 0x6f, 0x57, 0xcc, 0x6e, 0x44, 0xc4, 0x27, 0xbf,
0xc3, 0xdd, 0x19, 0x9e, 0x81, 0x16, 0xe2, 0x8f, 0x65, 0x34, 0xa7, 0x0f,
0x22, 0xba, 0xbf, 0x79, 0x57, 0x02, 0x81, 0x80, 0x2e, 0x21, 0x0e, 0xc9,
0xb5, 0xad, 0x31, 0xd4, 0x76, 0x0f, 0x9b, 0x0f, 0x2e, 0x70, 0x33, 0x54,
0x03, 0x58, 0xa7, 0xf1, 0x6d, 0x35, 0x57, 0xbb, 0x53, 0x66, 0xb4, 0xb6,
0x96, 0xa1, 0xea, 0xd9, 0xcd, 0xe9, 0x23, 0x9f, 0x35, 0x17, 0xef, 0x5c,
0xb8, 0x59, 0xce, 0xb7, 0x3c, 0x35, 0xaa, 0x42, 0x82, 0x3f, 0x00, 0x96,
0xd5, 0x9d, 0xc7, 0xab, 0xec, 0xec, 0x04, 0xb5, 0x15, 0xc8, 0x40, 0xa4,
0x85, 0x9d, 0x20, 0x56, 0xaf, 0x03, 0x8f, 0x17, 0xb0, 0xf1, 0x96, 0x22,
0x3a, 0xa5, 0xfa, 0x58, 0x3b, 0x01, 0xf9, 0xae, 0xb3, 0x83, 0x6f, 0x44,
0xd3, 0x14, 0x2d, 0xb6, 0x6e, 0xd2, 0x9d, 0x39, 0x0c, 0x12, 0x1d, 0x23,
0xea, 0x19, 0xcb, 0xbb, 0xe0, 0xcd, 0x89, 0x15, 0x9a, 0xf5, 0xe4, 0xec,
0x41, 0x06, 0x30, 0x16, 0x58, 0xea, 0xfa, 0x31, 0xc1, 0xb8, 0x8e, 0x08,
0x84, 0xaa, 0x3b, 0x19, 0x02, 0x81, 0x80, 0x70, 0x4c, 0xf8, 0x6e, 0x86,
0xed, 0xd6, 0x85, 0xd4, 0xba, 0xf4, 0xd0, 0x3a, 0x32, 0x2d, 0x40, 0xb5,
0x78, 0xb8, 0x5a, 0xf9, 0xc5, 0x98, 0x08, 0xe5, 0xc0, 0xab, 0xb2, 0x4c,
0x5c, 0xa2, 0x2b, 0x46, 0x9b, 0x3e, 0xe0, 0x0d, 0x49, 0x50, 0xbf, 0xe2,
0xa1, 0xb1, 0x86, 0x59, 0x6e, 0x7b, 0x76, 0x6e, 0xee, 0x3b, 0xb6, 0x6d,
0x22, 0xfb, 0xb1, 0x68, 0xc7, 0xec, 0xb1, 0x95, 0x9b, 0x21, 0x0b, 0xb7,
0x2a, 0x71, 0xeb, 0xa2, 0xb2, 0x58, 0xac, 0x6d, 0x5f, 0x24, 0xd3, 0x79,
0x42, 0xd2, 0xf7, 0x35, 0xdc, 0xfc, 0x0e, 0x95, 0x60, 0xb7, 0x85, 0x7f,
0xf9, 0x72, 0x8e, 0x4a, 0x11, 0xc3, 0xc2, 0x09, 0x40, 0x5c, 0x7c, 0x43,
0x12, 0x34, 0xac, 0x59, 0x99, 0x76, 0x34, 0xcf,

```

```

0x20, 0x88, 0xb0, 0xfb, 0x39, 0x62, 0x3a, 0x9b, 0x03, 0xa6, 0x84, 0x2c,
0x03, 0x5c, 0x0c, 0xca, 0x33, 0x85, 0xf5, 0x02, 0x81, 0x80, 0x56,
0x99, 0xe9, 0x17, 0xdc, 0x33, 0xe1, 0x33, 0x8d, 0x5c, 0xba, 0x17, 0x32,
0xb7, 0x8c, 0xbd, 0x4b, 0x7f, 0x42, 0x3a, 0x79, 0x90, 0xe3, 0x70,
0xe3, 0x27, 0xce, 0x22, 0x59, 0x02, 0xc0, 0xb1, 0x0e, 0x57, 0xf5, 0xdf,
0x07, 0xbf, 0xf8, 0x4e, 0x10, 0xef, 0x2a, 0x62, 0x30, 0x03, 0xd4,
0x80, 0xcf, 0x20, 0x84, 0x25, 0x66, 0x3f, 0xc7, 0x4f, 0x56, 0x8c, 0x1e,
0xe1, 0x18, 0x91, 0xc1, 0xfd, 0x71, 0x5f, 0x65, 0x9b, 0xe4, 0x4f,
0xe0, 0x1a, 0x3a, 0xf8, 0xc1, 0x69, 0xdb, 0xd3, 0xbb, 0x8d, 0x91, 0xd1,
0x11, 0x4f, 0x7e, 0x91, 0x1b, 0xb4, 0x27, 0xa5, 0xab, 0x7c, 0x7b,
0x76, 0xd4, 0x78, 0xfe, 0x63, 0x44, 0x63, 0x7e, 0xe3, 0xa6, 0x60, 0x4f,
0xb9, 0x55, 0x28, 0xba, 0xba, 0x83, 0x1a, 0x2d, 0x43, 0xd5, 0xf7,
0x2e, 0xe0, 0xfc, 0xa8, 0x14, 0x9b, 0x91, 0x2a, 0x36, 0xbf, 0xc7, 0x14

```

The example above contains the exponent, the modulus, and private key material.

Other Formats of Key Material

The format of key material depends on the application, and is therefore unpredictable. Key material commonly exists in any of the following formats; ASN1, PEM, P12, PFX, etc. Key material in those formats, or in another format, can likely be re-formatted to be acceptable for moving onto the SafeNet Luna PCIe HSM.

Sample Program

The sample program below encrypts a known RSA private key, then unwraps the key pair onto the SafeNet Luna PCIe HSM Partition.

```

/*****\
*
* File: UnwrapKey.cpp*
* Encrypts a PrivateKeyInfo structure with a generated DES
  key and then
* unwraps the RSA key onto a token.
*
* This file is provided as an example only.
*
* Copyright (C) 2017, Gemalto, Inc.
*
* All rights reserved. This file contains information that
  is
* proprietary to SafeNet, Inc. and may not be
* distributed or copied without written consent from
* SafeNet, Inc.
*
\*****/
#ifdef UNIX
#define _POSIX_SOURCE 1
#endif
#ifdef USING_STATIC_CHRYSTOKI
# define STATIC ckdemo_cpp
#endif
#include <assert.h>
#include <iostream.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <fcntl.h>
#include <sys/stat.h>
#include <time.h>

```



```

    }
    protectedInfo;
//Disclaimer
    cout
    << "\n\n\n\n";
cout << "THE SOFTWARE IS PROVIDED BY SAFENET INCORPORATED
(SAFENET) ON AN 'AS IS' BASIS, \n";
cout << "WITHOUT ANY OTHER WARRANTIES OR CONDITIONS,
EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED \n";
cout << "TO, WARRANTIES OF MERCHANTABILITY QUALITY,
SATISFACTORY QUALITY, MERCHANTABILITY OR FITNESS FOR\n";
cout << "A PARTICULAR PURPOSE, OR THOSE ARISING
BY LAW, STATUTE, USAGE OF TRADE, COURSE OF DEALING OR\n";
cout << "OTHERWISE. SAFENET
DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR \n";
cout << "THAT OPERATION OF THE SOFTWARE WILL BE
UNINTERRUPTED OR THAT THE SOFTWARE WILL BE ERROR-FREE.\n";
cout << "YOU ASSUME THE ENTIRE RISK AS TO THE
RESULTS AND PERFORMANCE OF THE SOFTWARE. NEITHER
\n";
cout << "SAFENET NOR OUR LICENSORS, DEALERS OR
SUPPLIERS SHALL HAVE ANY LIABILITY TO YOU OR ANY\n";
cout << "OTHER PERSON OR ENTITY FOR ANY INDIRECT,
INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, \n";
cout << "EXEMPLARY OR ANY OTHER DAMAGES WHATSOEVER,
INCLUDING, BUT NOT LIMITED TO, LOSS OF REVENUE OR \n";
cout << "PROFIT, LOST OR DAMAGED DATA, LOSS OF
USE OR OTHER COMMERCIAL OR ECONOMIC LOSS, EVEN IF \n";
cout << "SAFENET HAS BEEN ADVISED OF THE POSSIBILITY
OF SUCH DAMAGES, OR THEY ARE FORESEEABLE. \n";
cout << "SAFENET IS ALSO NOT RESPONSIBLE FOR CLAIMS
BY A THIRD PARTY. THE
MAXIMUM AGGREGATE \n";
cout << "LIABILITY OF SAFENET TO YOU AND THAT
OF SAFENET'S LICENSORS, DEALERS AND SUPPLIERS \n";
cout << "SHALL NOT EXCEED FORTY DOLLARS ($40.00CDN).
THE LIMITATIONS
IN THIS SECTION SHALL APPLY \n";
cout << "WHETHER OR NOT THE ALLEGED BREACH OR
DEFAULT IS A BREACH OF A FUNDAMENTAL CONDITION OR TERM \n";
cout << "OR A FUNDAMENTAL BREACH. SOME
STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF\n";
cout << "LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL
DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO \n";
cout << "YOU.\n";
cout << "THE LIMITED WARRANTY, EXCLUSIVE REMEDIES
AND LIMITED LIABILITY SET OUT HEREIN ARE FUNDAMENTAL \n";
cout << "ELEMENTS OF THE BASIS OF THE BARGAIN
BETWEEN YOU AND SAFENET. \n";
cout << "NO SUPPORT. YOU
ACKNOWLEDGE AND AGREE THAT THERE ARE NO SUPPORT SERVICES PROVIDED BY SAFENET\n";
cout << "INCORPORATED FOR THIS SOFTWARE\n"
<< endl;
//
Display Generic Warning
    cout
    << "\nInsert a token for the test...";
    cout
    << "\n\nWARNING!!! This test initializes the first ";

```

```

    cout
    << " token detected in the card reader.";
    cout
    << "\nDo not use a token that you don't want erased.";
    cout
    << "\nYou can use CTRL-C to abort now...Otherwise...";
    cout
    << "\n\n... press <Enter> key to continue ...\n";
    cout.flush();
    getchar();
    // Wait for keyboard hit
#ifdef STATIC
    //
    Connect to Chrystoki
    if(!ChrystokiConnect())
    {
    cout << "\n" "Unable to connect to Chrystoki.
        Error =
        " << LibError() << "\n";
    error = -1;
        goto
        exit_routine_1;
    }
#endif
    //
    Verify this is the version of the library required
    retCode
    = C_GetInfo(&protectedInfo.info);
    if(
    retCode != CKR_OK )
    {
        cout
        << endl << "Unable to call C_GetInfo() before C_Initialize()\n";
    error = -2;
        goto
        exit_routine_2;
    }
    else
    {
        CK_BYTE
        majorVersion = protectedInfo.info.version.major;
        CK_BYTE
        expectedVersion;
#ifdef PKCS11_2_0
        expectedVersion
        = 1;
#else
        expectedVersion
        = 2;
#endif
        if(
        expectedVersion != majorVersion )
        {
            cout
            << endl << "This version of the program was built for
                Cryptoki version "
                <<
                (int)expectedVersion << ".\n"
                <<
                "The loaded Cryptoki library reports its version to be "

```

```

        <<
(int)majorVersion << ".\n"
        <<
"Program will terminate.\n";
        //
Wait to exit until user read message and acknowledges
        cout
<< endl << "Press <Enter> key to end.";
        getchar();
// Wait for keyboard hit
        error
= -3;
        goto
exit_routine_2;
    }
}
//
Initialize the Library
retCode = C_Initialize(NULL);
if(retCode != CKR_OK)
{
cout << "\n" "Error 0x" <<
hex << retCode << " initializing cryptoki.\n";
error = -4;
        goto
exit_routine_3;
}
// Get the number of tokens possibly available
retCode = C_GetSlotList(TRUE, NULL, &usNumberOfSlots);
if(retCode != CKR_OK)
{
cout << "\n" "Error 0x" <<
hex << retCode << " getting slot list.\n";
error = -5;
        goto
exit_routine_3;
}
// Are any tokens present?
if(usNumberOfSlots == 0)
{
cout << "\n" "No tokens found\n";
error = -6;
        goto
exit_routine_3;
}
//
Get a list of slots
pSlotList = new CK_SLOT_ID[usNumberOfSlots];
retCode = C_GetSlotList(TRUE, pSlotList, &usNumberOfSlots);
if(retCode != CKR_OK)
{
cout << "\n" "Error 0x" <<
hex << retCode << " getting slot list.\n";
error = -7;
        goto
exit_routine_4;
}
//
Open a session
retCode = C_OpenSession(pSlotList[0], CKF_RW_SESSION | CKF_SERIAL_SESSION,

```

```

    NULL,
    NULL, &hSessionHandle);
if(retCode != CKR_OK)
{
cout << "\n" "Error 0x" <<
    hex << retCode << " opening session.\n";
error = -9;
    goto
    exit_routine_4;
}
Pinlogin(hSessionHandle);
if(retCode != CKR_OK)
{
cout << "\n" "Error 0x" <<
    hex << retCode << " Calling PinLogin fn";
exit(hSessionHandle);
}
//
Encrypt an RSA Key and then unwrap it onto the token
{
    //
    The following is an RSA Key that is formatted as a PrivateKeyInfo structure
    //BER
    encoded format
    const
    CK_BYTE pRsaKey[] = {
    0x30,
    0x82, 0x04, 0xbc, 0x02, 0x01, 0x00, 0x30, 0x0d, 0x06, 0x09, 0x2a, 0x86,
    0x48, 0x86, 0xf7, 0x0d, 0x01, 0x01,
    0x01, 0x05, 0x00, 0x04,
    0x82,
    0x04, 0xa6, 0x30, 0x82, 0x04, 0xa2, 0x02, 0x01, 0x00, 0x02, 0x82, 0x01,
    0x01, 0x00, 0xb8, 0xb5, 0x0f, 0x49,
    0x46, 0xb5, 0x5d, 0x58,
    0x04,
    0x8e, 0x52, 0x59, 0x39, 0xdf, 0xd6, 0x29, 0x45, 0x6b, 0x6c, 0x96, 0xbb,
    0xab, 0xa5, 0x6f, 0x72, 0x1b, 0x16,
    0x96, 0x74, 0xd5, 0xf9,
    0xb4,
    0x41, 0xa3, 0x7c, 0xe1, 0x94, 0x73, 0x4b, 0xa7, 0x23, 0xff, 0x61, 0xeb,
    0xce, 0x5a, 0xe7, 0x7f, 0xe3, 0x74,
    0xe8, 0x52, 0x5b, 0xd6,
    0x5d,
    0x5c, 0xdc, 0x98, 0x49, 0xfe, 0x51, 0xc2, 0x7e, 0x8f, 0x3b, 0x37, 0x5c,
    0xb3, 0x11, 0xed, 0x85, 0x91, 0x15,
    0x92, 0x24, 0xd8, 0xf1,
    0x7b,
    0x3d, 0x2f, 0x8b, 0xcd, 0x1b, 0x30, 0x14, 0xa3, 0x6b, 0x1b, 0x4d, 0x27,
    0xff, 0x6a, 0x58, 0x84, 0x9e, 0x79,
    0x94, 0xca, 0x78, 0x64,
    0x01,
    0x33, 0xc3, 0x58, 0xfc, 0xd3, 0x83, 0xeb, 0x2f, 0xab, 0x6f, 0x85, 0x5a,
    0x38, 0x41, 0x3d, 0x73, 0x20, 0x1b,
    0x82, 0xbc, 0x7e, 0x76,
    0xde,
    0x5c, 0xfe, 0x42, 0xd6, 0x7b, 0x86, 0x4f, 0x79, 0x78, 0x29, 0x82, 0x87,
    0xa6, 0x24, 0x43, 0x39, 0x74, 0xfe,
    0xf2, 0x0c, 0x08, 0xbe,

```

```

0xfa,
0x1e, 0x0a, 0x48, 0x6f, 0x14, 0x86, 0xc5, 0xcd, 0x9a, 0x98, 0x09, 0x2d,
0xf3, 0xf3, 0x5a, 0x7a, 0xa4, 0xe6,
0x8a, 0x2e, 0x49, 0x8a, 0xde, 0x73, 0xe9, 0x37, 0xa0, 0x5b,
0xef,
0xd0,
0xe0, 0x13, 0xac, 0x88, 0x5f, 0x59, 0x47, 0x96, 0x7f, 0x78, 0x18, 0x0e,
0x44, 0x6a, 0x5d, 0xec, 0x6e, 0xed,
0x4f, 0xf6, 0x6a, 0x7a,
0x58,
0x6b, 0xfe, 0x6c, 0x5a, 0xb9, 0xd2, 0x22, 0x3a, 0x1f, 0xdf, 0xc3, 0x09,
0x3f, 0x6b, 0x2e, 0xf1, 0x6d, 0xc3,
0xfb, 0x4e, 0xd4, 0xf2,
0xa3,
0x94, 0x13, 0xb0, 0xbf, 0x1e, 0x06, 0x2e, 0x29, 0x55, 0x00, 0xaa, 0x98,
0xd9, 0xe8, 0x77, 0x84, 0x8b, 0x3f,
0x5f, 0x5e, 0xf7, 0xf8,
0xa7,
0xe6, 0x02, 0xd2, 0x18, 0xb0, 0x52, 0xd0, 0x37, 0x2e, 0x53, 0x02, 0x03,
0x01, 0x00, 0x01, 0x02, 0x82, 0x01,
0x00, 0x0c, 0xdf, 0xd1,
0xe8,
0xf1, 0x9c, 0xc2, 0x9c, 0xd7, 0xf4, 0x73, 0x98, 0xf4, 0x87, 0xbd, 0x8d,
0xb2, 0xe1, 0x01, 0xf8, 0x9f, 0xac,
0x1f, 0x23, 0xdd, 0x78,
0x35,
0xe2, 0xd6, 0xd1, 0xf3, 0x4d, 0xb5, 0x25, 0x88, 0x16, 0xd1, 0x1a, 0x18,
0x33, 0xd6, 0x36, 0x7e, 0xc4, 0xc8,
0xe5, 0x5d, 0x2d, 0x74,
0xd5,
0x39, 0x3c, 0x44, 0x5a, 0x74, 0xb7, 0x7c, 0x48, 0xc1, 0x1f, 0x90, 0xe3,
0x55, 0x9e, 0xf6, 0x29, 0xad, 0xb4,
0x6d, 0x93, 0x78, 0xb3,
0xdc,
0x25, 0x0b, 0x9c, 0x73, 0x78, 0x7b, 0x93, 0x4c, 0xd3, 0x47, 0x09, 0xda,
0xe6, 0x69, 0x18, 0xc6, 0x0f, 0xfb,
0xa5, 0x95, 0xf5, 0xe8,
0x75,
0xe1, 0x01, 0x1b, 0xd3, 0x1c, 0xa2, 0x57, 0x03, 0x64, 0xdb, 0xf9, 0x5d,
0xf3, 0x3c, 0xa7, 0xd1, 0x4b, 0xb0,
0x90, 0x1b, 0x90, 0x62,
0xb4,
0x88, 0x30, 0x4b, 0x40, 0x4d, 0xcf, 0x7d, 0x89, 0x7a, 0xfb, 0x29, 0xc9,
0x64, 0x34, 0x0a, 0x52, 0xf6, 0x70,
0x7c, 0x76, 0x5a, 0x2e,
0x8f,
0x50, 0xd4, 0x92, 0x15, 0x97, 0xed, 0x4c, 0x2e, 0xf2, 0x3a, 0xd0, 0x58,
0x7e, 0xdb, 0xf1, 0xf4, 0xdd, 0x07,
0x76, 0x04, 0xf0, 0x55,
0x8b,
0x72, 0x2b, 0xa7, 0xa8, 0x78, 0x78, 0x67, 0xe6, 0xd8, 0xa5, 0xde, 0xe7,
0xc9, 0x1f, 0x5a, 0xa0, 0x89, 0xc7,
0x24, 0xa2, 0x71, 0xb6,
0x7b,
0x3b, 0xe6, 0x92, 0x69, 0x22, 0xaa, 0xe2, 0x47, 0x4b, 0x80, 0x3f, 0x6a,
0xab, 0xce, 0x4e, 0xcd, 0xe8, 0x94,
0x6c, 0xf7, 0x84, 0x73,
0x85,
0xfd, 0x85, 0x1d, 0xae, 0x81, 0xf7, 0xec, 0x12, 0x31, 0x7d, 0xc1, 0x99,
0xc0, 0x3c, 0x51, 0xb0, 0xdc, 0xb0,

```

```

0xba, 0x9c, 0x84, 0xb8,
0x70,
0xc2, 0x09, 0x7f, 0x96, 0x3d, 0xa1, 0xe2, 0x64, 0x27, 0x7a, 0x22, 0xb8,
0x75, 0xb9, 0xd1, 0x5f, 0xa5, 0x23,
0xf9, 0x62, 0xe0, 0x41,
0x02,
0x81, 0x81, 0x00, 0xf4, 0xf3, 0x08, 0xcf, 0x83, 0xb0, 0xab, 0xf2, 0x0f,
0x1a, 0x08, 0xaf, 0xc2, 0x42, 0x29,
0xa7, 0x9c, 0x5e, 0x52,
0x19,
0x69, 0x8d, 0x5b, 0x52, 0x29, 0x9c, 0x06, 0x6a, 0x5a, 0x32, 0x8f, 0x08,
0x45, 0x6c, 0x43, 0xb5, 0xac, 0xc3,
0xbb, 0x90, 0x7b, 0xec,
0xbb,
0x5d, 0x71, 0x25, 0x82, 0xf8, 0x40, 0xbf, 0x38, 0x00, 0x20, 0xf3, 0x8a,
0x38, 0x43, 0xde, 0x04, 0x41, 0x19,
0x5f, 0xeb, 0xb0, 0x50,
0x59,
0x10, 0xe1, 0x54, 0x62, 0x5c, 0x93, 0xd9, 0xdc, 0x63, 0x24, 0xd0, 0x17,
0x00, 0xc0, 0x44, 0x3e, 0xfc, 0xd1,
0xda, 0x4b, 0x24, 0xf7,
0xcb,
0x16, 0x35, 0xe6, 0x9f, 0x67, 0x96, 0x5f, 0xb0, 0x94, 0xde, 0xfa, 0xa1,
0xfd, 0x8c, 0x8a, 0xd1, 0x5c, 0x02,
0x8d, 0xe0, 0xa0, 0xa0,
0x02,
0x1d, 0x56, 0xaf, 0x13, 0x3a, 0x65, 0x5e, 0x8e, 0xde, 0xd1, 0xa8, 0x28,
0x8b, 0x71, 0xc9, 0x65, 0x02, 0x81,
0x81, 0x00, 0xc1, 0x0a,
0x47,
0x39, 0x91, 0x06, 0x1e, 0xb9, 0x43, 0x7c, 0x9e, 0x97, 0xc5, 0x09, 0x08,
0xbc, 0x22, 0x47, 0xe2, 0x96, 0x8e,
0x1c, 0x74, 0x80, 0x50,
0x6c,
0x9f, 0xef, 0x2f, 0xe5, 0x06, 0x3e, 0x73, 0x66, 0x76, 0x02, 0xbd, 0x9a,
0x1c, 0xfc, 0xf9, 0x6a, 0xb8, 0xf9,
0x36, 0x15, 0xb5, 0x20,
0x0b,
0x6b, 0x54, 0x83, 0x9c, 0x86, 0xba, 0x13, 0xb7, 0x99, 0x54, 0xa0, 0x93,
0x0d, 0xd6, 0x1e, 0xc1, 0x12, 0x72,
0x0d, 0xea, 0xb0, 0x14,
0x30,
0x70, 0x73, 0xef, 0x6b, 0x4c, 0xae, 0xb6, 0xff, 0xd4, 0xbb, 0x89, 0xa1,
0xec, 0xca, 0xa6, 0xe9, 0x95, 0x56,
0xac, 0xe2, 0x9b, 0x97,
0x2f,
0x2c, 0xdf, 0xa3, 0x6e, 0x59, 0xff, 0xcd, 0x3c, 0x6f, 0x57, 0xcc, 0x6e,
0x44, 0xc4, 0x27, 0xbf, 0xc3, 0xdd,
0x19, 0x9e, 0x81, 0x16,
0xe2,
0x8f, 0x65, 0x34, 0xa7, 0x0f, 0x22, 0xba, 0xbf, 0x79, 0x57, 0x02, 0x81,
0x80, 0x2e, 0x21, 0x0e, 0xc9, 0xb5,
0xad, 0x31, 0xd4, 0x76,
0x0f,
0x9b, 0x0f, 0x2e, 0x70, 0x33, 0x54, 0x03, 0x58, 0xa7, 0xf1, 0x6d, 0x35,
0x57, 0xbb, 0x53, 0x66, 0xb4, 0xb6,
0x96, 0xa1, 0xea, 0xd9,
0xcd,
0xe9, 0x23, 0x9f, 0x35, 0x17, 0xef, 0x5c, 0xb8, 0x59, 0xce, 0xb7, 0x3c,
0x35, 0xaa, 0x42, 0x82, 0x3f, 0x00,

```

```

0x96, 0xd5, 0x9d, 0xc7,
0xab,
0xec, 0xec, 0x04, 0xb5, 0x15, 0xc8, 0x40, 0xa4, 0x85, 0x9d, 0x20, 0x56,
0xaf, 0x03, 0x8f, 0x17, 0xb0, 0xf1,
0x96, 0x22, 0x3a, 0xa5,
0xfa,
0x58, 0x3b, 0x01, 0xf9, 0xae, 0xb3, 0x83, 0x6f, 0x44, 0xd3, 0x14, 0x2d,
0xb6, 0x6e, 0xd2, 0x9d, 0x39, 0x0c,
0x12, 0x1d, 0x23, 0xea,
0x19,
0xcb, 0xbb, 0xe0, 0xcd, 0x89, 0x15, 0x9a, 0xf5, 0xe4, 0xec, 0x41, 0x06,
0x30, 0x16, 0x58, 0xea, 0xfa, 0x31,
0xc1, 0xb8, 0x8e, 0x08,
0x84,
0xaa, 0x3b, 0x19, 0x02, 0x81, 0x80, 0x70, 0x4c, 0xf8, 0x6e, 0x86, 0xed,
0xd6, 0x85, 0xd4, 0xba, 0xf4, 0xd0,
0x3a, 0x32, 0x2d, 0x40,
0xb5,
0x78, 0xb8, 0x5a, 0xf9, 0xc5, 0x98, 0x08, 0xe5, 0xc0, 0xab, 0xb2, 0x4c,
0x5c, 0xa2, 0x2b, 0x46, 0x9b, 0x3e,
0xe0, 0x0d, 0x49, 0x50,
0xbf,
0xe2, 0xa1, 0xb1, 0x86, 0x59, 0x6e, 0x7b, 0x76, 0x6e, 0xee, 0x3b, 0xb6,
0x6d, 0x22, 0xfb, 0xb1, 0x68, 0xc7,
0xec, 0xb1, 0x95, 0x9b,
0x21,
0x0b, 0xb7, 0x2a, 0x71, 0xeb, 0xa2, 0xb2, 0x58, 0xac, 0x6d, 0x5f, 0x24,
0xd3, 0x79, 0x42, 0xd2, 0xf7, 0x35,
0xdc, 0xfc, 0x0e, 0x95,
0x60,
0xb7, 0x85, 0x7f, 0xf9, 0x72, 0x8e, 0x4a, 0x11, 0xc3, 0xc2, 0x09, 0x40,
0x5c, 0x7c, 0x43, 0x12, 0x34, 0xac,
0x59, 0x99, 0x76, 0x34,
0xcf,
0x20, 0x88, 0xb0, 0xfb, 0x39, 0x62, 0x3a, 0x9b, 0x03, 0xa6, 0x84, 0x2c,
0x03, 0x5c, 0x0c, 0xca, 0x33, 0x85,
0xf5, 0x02, 0x81, 0x80,
0x56,
0x99, 0xe9, 0x17, 0xdc, 0x33, 0xe1, 0x33, 0x8d, 0x5c, 0xba, 0x17, 0x32,
0xb7, 0x8c, 0xbd, 0x4b, 0x7f, 0x42,
0x3a, 0x79, 0x90, 0xe3,
0x70,
0xe3, 0x27, 0xce, 0x22, 0x59, 0x02, 0xc0, 0xb1, 0x0e, 0x57, 0xf5, 0xdf,
0x07, 0xbf, 0xf8, 0x4e, 0x10, 0xef,
0x2a, 0x62, 0x30, 0x03,
0xd4,
0x80, 0xcf, 0x20, 0x84, 0x25, 0x66, 0x3f, 0xc7, 0x4f, 0x56, 0x8c, 0x1e,
0xe1, 0x18, 0x91, 0xc1, 0xfd, 0x71,
0x5f, 0x65, 0x9b, 0xe4,
0x4f,
0xe0, 0x1a, 0x3a, 0xf8, 0xc1, 0x69, 0xdb, 0xd3, 0xbb, 0x8d, 0x91, 0xd1,
0x11, 0x4f, 0x7e, 0x91, 0x1b, 0xb4,
0x27, 0xa5, 0xab, 0x7c,
0x7b,
0x76, 0xd4, 0x78, 0xfe, 0x63, 0x44, 0x63, 0x7e, 0xe3, 0xa6, 0x60, 0x4f,
0xb9, 0x55, 0x28, 0xba, 0xba, 0x83,
0x1a, 0x2d, 0x43, 0xd5,
0xf7,
0x2e, 0xe0, 0xfc, 0xa8, 0x14, 0x9b, 0x91, 0x2a, 0x36, 0xbf, 0xc7, 0x14
};

```

```

CK_BYTE
    knownRSA1Modulus[]
    = {
0xb8, 0xb5, 0x0f, 0x49, 0x46, 0xb5, 0x5d, 0x58, 0x04, 0x8e,
    0x52, 0x59, 0x39, 0xdf, 0xd6,
0x29,
0x45, 0x6b, 0x6c, 0x96, 0xbb, 0xab, 0xa5, 0x6f, 0x72, 0x1b,
    0x16, 0x96, 0x74, 0xd5, 0xf9,
0xb4,
0x41, 0xa3, 0x7c, 0xe1, 0x94, 0x73, 0x4b, 0xa7, 0x23, 0xff,
    0x61, 0xeb, 0xce, 0x5a, 0xe7,
0x7f,
0xe3, 0x74, 0xe8, 0x52, 0x5b, 0xd6, 0x5d, 0x5c, 0xdc, 0x98,
    0x49, 0xfe, 0x51, 0xc2, 0x7e,
0x8f,
0x3b, 0x37, 0x5c, 0xb3, 0x11, 0xed, 0x85, 0x91, 0x15, 0x92,
    0x24, 0xd8, 0xf1, 0x7b, 0x3d,
0x2f,
0x8b, 0xcd, 0x1b, 0x30, 0x14, 0xa3, 0x6b, 0x1b, 0x4d, 0x27,
    0xff, 0x6a, 0x58, 0x84, 0x9e,
0x79,
0x94, 0xca, 0x78, 0x64, 0x01, 0x33, 0xc3, 0x58, 0xfc, 0xd3,
    0x83, 0xeb, 0x2f, 0xab, 0x6f,
0x85,
0x5a, 0x38, 0x41, 0x3d, 0x73, 0x20, 0x1b, 0x82, 0xbc, 0x7e,
    0x76, 0xde, 0x5c, 0xfe, 0x42,
0xd6,
0x7b, 0x86, 0x4f, 0x79, 0x78, 0x29, 0x82, 0x87, 0xa6, 0x24,
    0x43, 0x39, 0x74, 0xfe, 0xf2,
0x0c,
0x08, 0xbe, 0xfa, 0x1e, 0x0a, 0x48, 0x6f, 0x14, 0x86, 0xc5,
    0xcd, 0x9a, 0x98, 0x09, 0x2d,
0xf3,
0xf3, 0x5a, 0x7a, 0xa4, 0xe6, 0x8a, 0x2e, 0x49, 0x8a, 0xde,
    0x73, 0xe9, 0x37, 0xa0, 0x5b,
0xef,
0xd0, 0xe0, 0x13, 0xac, 0x88, 0x5f, 0x59, 0x47, 0x96, 0x7f,
    0x78, 0x18, 0x0e, 0x44, 0x6a,
0x5d,
0xec, 0x6e, 0xed, 0x4f, 0xf6, 0x6a, 0x7a, 0x58, 0x6b, 0xfe,
    0x6c, 0x5a, 0xb9, 0xd2, 0x22,
0x3a,
0x1f, 0xdf, 0xc3, 0x09, 0x3f, 0x6b, 0x2e, 0xf1, 0x6d, 0xc3,
    0xfb, 0x4e, 0xd4, 0xf2, 0xa3,
0x94,
0x13, 0xb0, 0xbf, 0x1e, 0x06, 0x2e, 0x29, 0x55, 0x00, 0xaa,
    0x98, 0xd9, 0xe8, 0x77, 0x84,
0x8b,
0x3f, 0x5f, 0x5e, 0xf7, 0xf8, 0xa7, 0xe6, 0x02, 0xd2, 0x18,
    0xb0, 0x52, 0xd0, 0x37, 0x2e,
0x53,
    },
    knownRSA1PubExponent[]
    = { 0x01, 0x00, 0x01 };
    char
    *pPlainData = 0;
    unsigned
    long ulPlainDataLength;
    char
    *pEncryptedData = 0;

```

```

    unsigned
long ulEncryptedDataLength = 0;
    CK_MECHANISM
mech;
    CK_USHORT
    usStatus=0,
        usKeyLength;
    CK_OBJECT_HANDLE
hKey;
    CK_OBJECT_CLASS
    SymKeyClass
    = CKO_SECRET_KEY;
    CK_BBOOL
        bTrue
= 1,
        bFalse
= 0,
        bToken
= bTrue,
        bSensitive
= bTrue,
        bPrivate
= bTrue,
        bEncrypt
= bTrue,
        bDecrypt
= bTrue,
        bSign
= bFalse, // "...
        bVerify
= bFalse, //Will not allow sign/verify operation.
        bWrap
= bTrue,
        bUnwrap
= bTrue,
#ifdef EXTRACTABLE
        bExtract
= bTrue,
#endif //EXTRACTABLE
        bDerive
= bTrue;
    CK_KEY_TYPE
    keyType;
    CK_USHORT
    usValueBits;
    char
        pbPublicKeyLabel[128];
    CK_ATTRIBUTE_PTR
pPublicTemplate;
    CK_USHORT
usPublicTemplateSize = 0;
    char
iv[8] = { '1', '2', '3', '4', '5', '6', '7', '8' };
    CK_ATTRIBUTE
SymKeyTemplate[] = {
    {CKA_CLASS,
0, sizeof(SymKeyClass)},
    {CKA_KEY_TYPE,
0, sizeof(keyType)},

```

```

        {CKA_TOKEN,
0, sizeof(bToken)},
        {CKA_SENSITIVE,
0, sizeof(bSensitive)},
        {CKA_PRIVATE,
0, sizeof(bPrivate)},
        {CKA_ENCRYPT,
0, sizeof(bEncrypt)},
        {CKA_DECRYPT,
0, sizeof(bDecrypt)},
        {CKA_SIGN,
0, sizeof(bSign)},
        {CKA_VERIFY,
0, sizeof(bVerify)},
        {CKA_WRAP,
0, sizeof(bWrap)},
        {CKA_UNWRAP,
0, sizeof(bUnwrap)},
        {CKA_DERIVE,
0, sizeof(bDerive)},
        {CKA_VALUE_LEN, 0,
sizeof(usKeyLength)
},
        {CKA_LABEL,
0, 0} //
Always keep last!!!
#ifdef EXTRACTABLE //Conditional
stuff must be at the end!!!!
        {CKA_EXTRACTABLE,
0, sizeof(bExtract)},
#endif //EXTRACTABLE
    };
    CK_OBJECT_HANDLE
hUnWrappedKey, hPublicRSAKey;
    char
        *pbWrappedKey;
    unsigned
long    ulWrappedKeySize;
    CK_OBJECT_CLASS
privateKey
= CKO_PRIVATE_KEY,
publicKey = CKO_PUBLIC_KEY;
    CK_KEY_TYPE
rsaType
=
CKK_RSA;
    CK_BYTE
pLabel[]
= "RSA
private Key",
pbPublicRSAKeyLabel[] = "RSA Public Key";
    CK_ATTRIBUTE
*pTemplate;
    CK_ULONG
usTemplateSize,
ulPublicRSAKeyTemplateSize;
    CK_ATTRIBUTE
pPublicRSAKeyTemplate[] = {

```

```

        {CKA_CLASS,
0,
sizeof(publicKey) },
        {CKA_KEY_TYPE,
0,    sizeof(rsaType)
    },
        {CKA_TOKEN,
0,
sizeof(bToken)
    },
        {CKA_PRIVATE,
0,    sizeof(bPrivate)
    },
        {CKA_ENCRYPT,
0,    sizeof(bEncrypt)
    },
        {CKA_VERIFY,
0,
sizeof(bSign)
    },
        {CKA_WRAP,
0,
sizeof(bWrap)
    },
{CKA_MODULUS,
0, sizeof(knownRSA1Modulus) },
{CKA_PUBLIC_EXPONENT,
0, sizeof(knownRSA1PubExponent) },
        {CKA_LABEL,
0,
sizeof(pbPublicRSAKeyLabel)
    }
    };
    CK_ATTRIBUTE
pPrivateKeyTemplate[] = {
        {CKA_CLASS,
&privateKey,
sizeof(privateKey) },
        {CKA_KEY_TYPE,
&rsaType,    sizeof(rsaType)
    },
        {CKA_TOKEN,
&bToken,
sizeof(bToken)
    },
        {CKA_SENSITIVE, &bSensitive,
sizeof(bSensitive) },
        {CKA_PRIVATE,
&bPrivate,
sizeof(bPrivate)
    },
        {CKA_DECRYPT,
&bEncrypt,
sizeof(bEncrypt)
    },
        {CKA_SIGN,
&bSign,
sizeof(bSign)
    },

```

```

//{CKA_SIGN_RECOVER,
&bTrue, sizeof(bTrue)    },
    {CKA_UNWRAP,
    &bWrap,
    sizeof(bWrap)
    },
{CKA_EXTRACTABLE, &bFalse, sizeof(bFalse)    },
{CKA_LABEL,      pLabel,
    sizeof(pLabel)
    }
};
//
Generate a DES3 Key
    SymKeyTemplate[0].pValue
= &SymKeyClass;
    SymKeyTemplate[1].pValue
= &keyType;
    SymKeyTemplate[2].pValue
= &bToken;
    SymKeyTemplate[3].pValue
= &bSensitive;
    SymKeyTemplate[4].pValue
= &bPrivate;
    SymKeyTemplate[5].pValue
= &bEncrypt;
    SymKeyTemplate[6].pValue
= &bDecrypt;
    SymKeyTemplate[7].pValue
= &bSign;
    SymKeyTemplate[8].pValue
= &bVerify;
    SymKeyTemplate[9].pValue
= &bWrap;
    SymKeyTemplate[10].pValue
= &bUnwrap;
    SymKeyTemplate[11].pValue
= &bDerive;
    SymKeyTemplate[12].pValue
= &usKeyLength;
    SymKeyTemplate[13].pValue
= pbPublicKeyLabel;
#ifdef EXTRACTABLE
    SymKeyTemplate[14].pValue
= &bExtract;
#endif //EXTRACTABLE
    mech.mechanism
= CKM_DES3_KEY_GEN;
    mech.pParameter
= 0;
    mech.usParameterLen
= 0;
    keyType
= CKK_DES3;
    usKeyLength
= 24;
    strcpy(
pbPublicKeyLabel, "Generated DES3 Key" );
    pPublicTemplate
= SymKeyTemplate;

```

```

        usPublicTemplateSize
= DIM(SymKeyTemplate);
    //
Adjust size of label (ALWAYS LAST ENTRY IN ARRAY)
    pPublicTemplate[usPublicTemplateSize-1].usValueLen
= strlen(
pbPublicKeyLabel );
    retCode
= C_GenerateKey(    hSessionHandle,
                    (CK_MECHANISM_PTR)&mech,
                    pPublicTemplate,
                    usPublicTemplateSize,
                    &hKey);

    if(retCode
== CKR_OK)
    {
        cout
<< pbPublicKeyLabel << ": " << hKey <<
endl;
    }
    else
    {
        cout
<< "\n" "Error 0x" << hex << retCode;
        cout
<< " generating the DES3 Key.\n";
        error
= -11;
        goto
exit_routine_6;
    }
    //
Encrypt the RSA Key
    mech.mechanism
= CKM_DES3_CBC;
    mech.pParameter
= iv;
    mech.usParameterLen
= sizeof(iv);
    pPlainData
= (char *) (pRsaKey);
    ulPlainDataLength
= sizeof(pRsaKey);
    //
Allocate memory for output buffer
    if(
retCode == CKR_OK )
    {
        pEncryptedData
= new char [ulPlainDataLength + 2048]; // Leave
// extra room for
// RSA Operations
        if(
!pEncryptedData )
        {
            retCode
= CKR_DEVICE_ERROR;
        }
    }
    //
Start encrypting

```

```

    if(
retCode == CKR_OK )
    {
        retCode
= C_EncryptInit(hSessionHandle, &mech, hKey);
    }
    //
Continue encrypting
    if(
retCode == CKR_OK )
    {
        CK_USHORT
usInDataLen,
                usOutDataLen
= (CK_USHORT) (ulPlainDataLength + 2048);
        CK_ULONG
ulBytesRemaining
= ulPlainDataLength;
        char
* pPlainTextPointer
= pPlainData;
        char
* pEncryptedDataPointer
= pEncryptedData;
        while
(ulBytesRemaining > 0)
        {
            if
(ulBytesRemaining > 0xfff0) // We are longer than a USHORT can handle
            {
                usInDataLen
= 0xfff0;
                ulBytesRemaining
-= usInDataLen;
            }
            else
            {
                usInDataLen
= (CK_USHORT) ulBytesRemaining;
                ulBytesRemaining
-= usInDataLen;
            }
            retCode
= C_EncryptUpdate( hSessionHandle,
                    (CK_BYTE_PTR)pPlainTextPointer,
                    usInDataLen,
                    (CK_BYTE_PTR)pEncryptedDataPointer,
                    &usOutDataLen
);
                pPlainTextPointer
+= usInDataLen;
                pEncryptedDataPointer
+= usOutDataLen;
                ulEncryptedDataLength
+= usOutDataLen;
            }
        }

    //
Finish encrypting

```

```

        if(
retCode == CKR_OK )
        {
            CK_USHORT
usOutDataLen;
            CK_BYTE_PTR
pOutData = (CK_BYTE_PTR)pEncryptedData;
            pOutData
+= ulEncryptedDataLength;
            retCode
= C_EncryptFinal(hSessionHandle, pOutData, &usOutDataLen);
            ulEncryptedDataLength
+= usOutDataLen;
        }
        else
        {
            cout
<< "\n" "Error 0x" << hex << retCode;
            cout
<< " somewhere in the encrypting.\n";
            if(
pEncryptedData )
            {
                delete
pEncryptedData;
            }
            error
= -12;
            goto
exit_routine_6;
        }
        mech.mechanism
=
CKM_DES3_CBC;
        mech.pParameter
=
(void*) "12345678"; // 8 byte IV
        mech.usParameterLen
= 8;
        pTemplate
= pPrivateKeyTemplate;
        usTemplateSize
= DIM(pPrivateKeyTemplate);
        pbWrappedKey
= pEncryptedData;
        ulWrappedKeySize
= ulEncryptedDataLength;
        if(
retCode == CKR_OK )
        {
            retCode
= C_UnwrapKey( hSessionHandle,
                &mech,
                hKey,
                (CK_BYTE_PTR)pbWrappedKey,
                (CK_USHORT)ulWrappedKeySize,
                pTemplate,
                usTemplateSize,
                &hUnWrappedKey);
        }
    }

```

```

//
Report unwrapped key handle
    if(
retCode == CKR_OK )
    {
        cout
<< "\n Private key Unwrapped key is:" << hUnWrappedKey
<< "\n\n";
    }
    else
    {
        cout
<< "\n" "Error 0x" << hex << retCode;
        cout
<< " unwrapping.\n";
        if(
pEncryptedData )
        {
            delete
pEncryptedData;
        }
        error
= -13;
        goto
exit_routine_6;
    }
//
Release temporary memory
    if(
pEncryptedData )
    {
        delete
pEncryptedData;
    }
//
Create the Public Key that goes with the Private Key
    if(
retCode == CKR_OK )
    {
//
Unwrap it onto the token
pPublicRSAKeyTemplate[0].pValue
= &publicKey;
pPublicRSAKeyTemplate[1].pValue
= &rsaType;
pPublicRSAKeyTemplate[2].pValue
= &bToken;
pPublicRSAKeyTemplate[3].pValue
= &bPrivate;
pPublicRSAKeyTemplate[4].pValue
= &bEncrypt;
pPublicRSAKeyTemplate[5].pValue
= &bSign;
pPublicRSAKeyTemplate[6].pValue
= &bWrap;
pPublicRSAKeyTemplate[7].pValue
= knownRSA1Modulus;
pPublicRSAKeyTemplate[8].pValue
= knownRSA1PubExponent;

```

```

    pPublicKeyTemplate[9].pValue
= pbPublicKeyLabel;
    pTemplate
= pPublicKeyTemplate;
    usTemplateSize
= DIM(pPublicKeyTemplate);
    retCode
= C_CreateObject( hSessionHandle,
pTemplate,
    usTemplateSize,
    &hPublicKey);
    if(retCode
== CKR_OK)
    {
    cout
<< pbPublicKeyLabel << ": " << hPublicKey
<< endl;
    }
    else
    {
    cout
<< "\n" "Error 0x" << hex << retCode;
    cout
<< " creating the RSA Public Key.\n";
    error
= -14;
    goto
    exit_routine_6;
    }
}
if( retCode == CKR_OK )
{
CK_CHAR label[] = "RSA Key";
CK_ATTRIBUTE RSAFindPriTemplate[] =
{
CKA_LABEL, label, sizeof(label)
};
CK_ULONG numHandles;
CK_OBJECT_HANDLE handles[1000];
retCode = C_FindObjectsInit( hSessionHandle, RSAFindPriTemplate,
1 );
if(retCode != CKR_OK)
{
cout << "C_FindObjectsInit not returning OK ("
<< hex << retCode << ")\n\n";
goto exit_routine_6;
}
retCode =C_FindObjects( hSessionHandle , handles, 90,
&numHandles );
if(retCode != CKR_OK)
{
cout << "C_FindObjects not returning OK ("
<< hex <<
retCode << ")\n\n";
goto exit_routine_6;
}
cout << "Everything's GOOD\n\n";
for(int i=0; i < numHandles; i++)
{
cout << handles[i] << "\n";
}
}

```

```

}
}
//CJM-> END OF TEST CODE
//
Beginning of exit routines
exit_routine_6:
//
Logout
retCode
= C_Logout(hSessionHandle);
if(retCode
!= CKR_OK)
{
cout << "\n" "Error 0x" <<
hex << retCode << " logging out.";
}
exit_routine_5:
// Close the session
retCode
= C_CloseSession(hSessionHandle);
if(retCode != CKR_OK)
{
cout << "\n" "Error 0x" <<
hex << retCode << " closing session.";
}
exit_routine_4:
delete
pSlotList;
exit_routine_3:
#ifdef PKCS11_2_0
C_Finalize(0);
#else
C_Terminate();
#endif
exit_routine_2:
#ifndef STATIC
//
No longer need Crystoki
CrystokiDisconnect();
#endif
exit_routine_1:
cout
<< "\nDone. (" << dec << error << ")\n";
cout.flush();
return
error;
}
CK_RV Pinlogin(CK_SESSION_HANDLE
hSession)
{

CK_RV retCode;
unsigned char buffer[MAX];
int count =0;
cout << "Please enter the USER password : "
<< endl;
//calling get PinString to mask input, variable "count"

//holds length of "buffer"(password)
//needed for Login call
count = getPinString(buffer);

```

```

//Login as user on token
in slot
retCode = C_Login(hSession, CKU_USER, buffer, count);
if(retCode != CKR_OK)
{
cout << "\n" "Error 0x" <<
hex << retCode;
cout
<< " logging in as user.";
exit(hSession);
return
-3;
}
cout << "logging into the token...";
cout << "\nlogged into token " << endl;
return retCode;
}
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
// getPnString()
// =====
//
// This function retrieves a pin string from the user. It
// modifies the
// console mode before starting so that the characters the
// user types are
// not echoed, and a '*' character is displayed for each
// typed character
// instead.
//
// Backspace is supported, but we don't get any fancier than
// that.
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
int getPnString(CK_CHAR_PTR pw)
{
int
len=0;
char
c=0;
//
Unfortunately, the method of turning off character echo is
// different for Windows and Unix platforms. So
we have to
// conditionally compile the appropriate section. Even
the basic
// password retrieval is slightly different, since
//
Windows and Unix use different character codes for the return key.
#ifdef WIN32
DWORD
mode;
//
This console mode stuff only applies to windows. We'll
have to
// do something else when it comes to unix.
if
(GetConsoleMode(GetStdHandle(STD_INPUT_HANDLE), &mode)) {
if
(SetConsoleMode(GetStdHandle(STD_INPUT_HANDLE), mode & (!ENABLE_ECHO_INPUT)))
{

```

```

        while
(c != '\r')
{
    //
wait for a character to be hit
    while
(!_kbhit()) {
        Sleep(100);
    }
    //
get it
    c
= _getch();
    //
check for carriage return
    if
(c != '\r') {
        //
check for backspace
        if
(c!='\b') {
            //
neither CR nor BS -- add it to the password string
            printf("*");
            *pw++
= c;
            len++;
        }
    else {
// handle backspace -- delete the last character &
// erase it from the screen
        if
(len > 0) {
            pw--;
            len--;
            printf("\b
\b");
        }
    }
}
//
Add the zero-termination
    *pw
= '\0';
    SetConsoleMode(GetStdHandle(STD_INPUT_HANDLE),
mode);
    printf("\n");
}
}
#endif
return
len;
}

```

Audit Logging

By default, the HSM logs select events. See "[Audit Logging](#)" on page 1 in the *Administration Guide* for more information.

The HSM creates a log secret unique to the HSM, computed during the first initialization after manufacture. The log secret resides in flash memory (permanent, non-volatile memory), and is used to create log records that are sent to a log file. Later, the log secret is used to prove that a log record originated from a legitimate HSM and has not been tampered with.

Audit Log Records

A log record consists of two fields – the log message and the HMAC for the previous record. When the HSM creates a log record, it uses the log secret to compute the SHA256-HMAC of all data contained in that log message, plus the HMAC of the previous log entry. The HMAC is stored in HSM flash memory. The log message is then transmitted, along with the HMAC of the previous record, to the host. The host has a logging daemon to receive and store the log data on the host hard drive.

For the first log message ever returned from the HSM to the host there is no previous record and, therefore, no HMAC in flash. In this case, the previous HMAC is set to zero and the first HMAC is computed over the first log message concatenated with 32 zero-bytes. The first record in the log file then consists of the first log message plus 32 zero-bytes. The second record consists of the second message plus HMAC1 = HMAC (message1 || 0x0000). This results in the organization shown below.

MSG 1	HMAC 0
	...
MSG n-1	HMAC n-2
MSG n	HMAC n-1
...	
MSG n+m	HMAC n+m-1
MSG n+m+1	HMAC n+m
...	
MSG end	HMAC n+m-1
Recent HMAC in NVRAM	HMAC end

To verify a sequence of m log records which is a subset of the complete log, starting at index n , the host must submit the data illustrated above. The HSM calculates the HMAC for each record the same way as it did when the record was originally generated, and compares this HMAC to the value it received. If all of the calculated HMACs match the received HMACs, then the entire sequence verifies. If an HMAC doesn't match, then the

The log message is “session 1 Access 2147483651:22621 operation LUNA_CREATE_CONTAINER returned LUNA_RET_SM_UNKNOWN_TOSM_STATE(0x00300014) (using PIN (entry=LUNA_ENTRY_DATA_AREA))”.

In the message text, the “who” is the session identified by “session 1 Access 2147483651:22621” (the application is identified by the access ID major = 2147483651, minor = 22621).

The “what” is “LUNA_CREATE_CONTAINER”.

The operation status is “LUNA_RET_SM_UNKNOWN_TOSM_STATE(0x00300014)”.

The HMAC of previous record is

“29C51014B6F131EC67CF48734101BBE301335C25F43EDF8828745C40755ABE25”.

The remainder is the raw data for this record as ASCII-HEX.

Log External

An important element of the security audit logging feature is the Log External function. This SafeNet extension to PKCS #11 allows a user application to insert text of the user’s choice into the log record stream. The function call is **CA_LogExternal ()**. It can be used, for example, to insert an application name or the name of the user who is logged into the application and have the inserted text string protected as part of the audit log in the same way as records that have been generated by the HSM itself. It is recommended that applications use the **CA_LogExternal ()** function when the application starts to insert the application name and also to insert the user name each time an individual user logs into or out of the application. The function is called as:

```
CA_LogExternal(CK_SLOT_ID slotID, CK_SESSION_HANDLE hSession, CK_CHAR_PTR pData, CK_ULONG puldataLen);
```

where:

- > **slotID** is PKCS #11 slot containing the HSM or partition being addressed
- > **hSession** is the handle of the session with which the record is to be associated
- > **pData** is the pointer to the character array containing the external message
- > **puldataLen** is the length of the character array

Note that the input character array is limited to a maximum of 100 characters and it will be truncated at 100 characters if **puldataLen** > 100.

For applications that cannot add this function call, it is possible to use the LunaCM command-line function **audit log external** within a startup script to insert a text record at the time the application is started.

When a user logs in to the SafeNet Luna PCIe HSM `lunash:> session`, the **CA_LogExternal ()** function is automatically called to register the user name and access ID. Subsequent HSM operations can be tracked by the access ID.

You must configure the “log external” event category in order for the HSM to log the **CA_LogExternal ()** messages.

CHAPTER 7: Java Interfaces

This chapter describes the Java interfaces to the PKCS#11 API. It contains the following topics:

- > ["SafeNet JSP Overview and Installation" below](#)
- > ["SafeNet JSP Configuration" on page 375](#)
- > ["The JCPROV PKCS#11 Java Wrapper" on page 379](#)
- > ["Java or JSP Errors" on page 385](#)
- > ["Re-Establishing a Connection Between Your Java Application and SafeNet Luna PCIe HSM" on page 386](#)
- > ["Recovering From the Loss of All HA Members" on page 386](#)
- > ["Using Java Keytool with SafeNet Luna PCIe HSM" on page 389](#)

SafeNet JSP Overview and Installation

The SafeNet JSP is part of an application program interface (API) that allows Java applications to make use of certain SafeNet products.

As with other APIs, some existing Java-based applications might have generic requirements and calls that can already work with SafeNet products. In other cases, it might be necessary for you or your vendor to create an application or to adapt one, using the JSP API.

You have the choice of:

- > using a previously integrated third-party application, known to work with this SafeNet product
- > performing your own integration with a Java-based application supplied by you or a third party, or
- > developing your own application using our Java API.

Develop your own Java apps using our included Software Development Kit, which includes SafeNet Java API usage notes for developers, as well as development support by SafeNet. A standard Java development environment is required, in addition to the API provided by SafeNet.

Please refer to the current-version SafeNet Luna PCIe HSM Customer Release Notes (CRN) for the most up-to-date list of supported platforms and APIs.

NOTE Java Provider (JSP) - both GMC and GMAC are supported. **GmacAesDemo.java** provides a sample for using GMAC with Java.

Java Parameter Specification class **LunaGmacParameterSpec.java** defines default values recommended by the NIST specification.

The following sections describe the tasks required to set up the JSP API:

- > ["Installation" on the next page](#)
- > ["JSP Registration" on page 372](#)

> ["Post-Installation Tasks" on page 373](#)

Installation

To use the SafeNet JavaSP service providers three main components are needed:

- > The Java SDK
- > The Java Cryptographic JCE Policy files (optional)
- > The SafeNet JavaSP artifacts in the SafeNet Luna HSM Client

Java SDK Installation

Acquire and install the JDK or JRE (available from the Java site, not included with the SafeNet software). Refer to the Customer Release Notes for supported Java versions.

Java Cryptographic JCE Policy Files Installation (optional)

If you intend to generate large key sizes, you might need to apply the unlimited strength ciphers policy. You will need two cryptographic JCE Policy files v 7/8/9/10/11 (available from the Oracle Java web site): `local_policy.jar` and `US_export_policy.jar`.

Copy these files to `JAVA_HOME/jre/lib/security` (or the equivalent directory that applies to your setup).

```
[root@my-client]# echo $JAVA_HOME
/usr/java/default
[root@my-client]# cp -p local_policy.jar /usr/java/default/jre/lib/security/
[root@my-sclient]# cp -p US_export_policy.jar /usr/java/default/jre/lib/security/
```

If you see errors like "Invalid Key size", that is usually an indication that the JCE is not properly installed.

SafeNet JavaSP included in the SafeNet Luna HSM Client

Follow the installation procedure for the SafeNet Luna HSM Client as described in the *Installation Guide*. When installing the SafeNet Luna HSM Client software, choose the option to install SafeNet JSP. There are two SafeNet files: the **LunaProvider.jar** file, and the Java library file (**libLunaAPI.so** in Unix based systems or **LunaAPI.dll** in Windows systems). To ensure that the Java Environment can find these files, follow the instructions for either Java 7/8 or Java 9+.

Operating System	JSP Install directory
AIX	<code>/usr/safenet/lunaclient/jsp/lib</code>
Linux	<code>/usr/safenet/lunaclient/jsp/lib</code>
Solaris	<code>/opt/safenet/lunaclient/jsp/</code>
Windows	<code>C:\Program Files\LunaClient\JSP\lib</code>

To configure Java 7/8 for SafeNet JSP

To ensure that SafeNet Luna PCIe HSM and SafeNet JSP can work with the JRE, copy the JSP files from the default installation location to the Java environment. The exact destination directory might differ depending on where you obtained your Java system, the version, and any choices that you made while installing and

configuring it.

Operating System	Destination directory example
AIX	<code>/usr/jre/lib/ext</code>
Linux	<code>/usr/jre/lib/ext</code>
Solaris	<code>/opt/jre/lib/ext</code>
Windows	<code><java_install_dir>\bin</code> <code>C:\Program Files\Java\jdk1.8.0_121\bin</code> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE Java 7/8/9 for Windows has removed the <code><java_install_dir>\lib\ext</code> directory from the Java library path.</p> </div>

To configure Java 9+ for SafeNet JSP

Add **LunaProvider.jar** to the Java classpath and specify the SafeNet Java library location (**libLunaAPI.so** in Unix based systems or **LunaAPI.dll** in Windows systems) in the Java library path.

For example:

```
> java -cp <directory_location>/LunaProvider.jar -Djava.library.path=<SafeNet_Java_library_location>
<class name>
```

TIP In Windows, you can also put **LunaAPI.dll** in an arbitrary folder and add that folder to the system path. Java will search the system path for **LunaAPI.dll**.

The exact directory might differ depending on where you obtained your Java system, the version, and any choices that you made while installing and configuring it.

JSP Registration

Before Java can use SafeNet JSP, you must register it with the Java Runtime Environment. You can choose either a static registration or a dynamic registration. A static registration defaults all Java applications to default to the SafeNet provider, while a dynamic registration allows you to set the provider for Java applications individually.

JSP Static Registration

NOTE This section applies to JSP, not to JC PROV.

You would choose static registration of providers if you want all applications to default to the SafeNet provider.

Once your client has externally logged in using **salogin** or your own HSM-aware utility, any application would be able to use SafeNet product without being designed to log in to the HSM Partition.

Edit the **java.security** file located in the **/jre/lib/security** directory of your Java SDK/JRE installation to read as follows:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.sun.net.ssl.internal.ssl.Provider
security.provider.3=com.safenetinc.luna.provider.LunaProvider
security.provider.4=com.sun.rsajca.Provider
security.provider.5=com.sun.crypto.provider.SunJCE
security.provider.6=sun.security.jgss.SunProvider
```

You can set our provider in first position for efficiency if SafeNet Luna HSM operations are your primary mode. However, if your application needs to perform operations not supported by the LunaProvider (secure random generation or random publickey verification, for example) then it would receive error messages from the HSM and would need to handle those gracefully before resorting to providers further down the list. We have found that having our provider in third position works well for most applications.

The modifications in the **java.security** file are global, and they might result in the breaking of another application that uses the default KeyPairGenerator without logging into the SafeNet Luna Network HSM first. This consideration might argue for using dynamic registration, instead.

JSP Dynamic Registration

You might prefer to employ dynamic registration of Providers, in order to avoid possible negative impacts on other applications running on the same machine. As well, the use of dynamic registration allows you to keep installation as straightforward as possible for your customers.

This sample code shows an example of dynamic registration with the SafeNet provider. The SafeNet provider is registered in position 2, ensuring that the "SUN" provider is still the default. If you want the SafeNet provider to be used when no provider is explicitly specified, it should be registered at position 1.

```
try {
    com.safenetinc.luna.LunaSlotManager.getInstance().login("<HSM Partition Password>");
    java.security.Provider provider = new com.safenetinc.luna.provider.LunaProvider();
    // removing the provider is only necessary if it is already registered
    // and you want to change its position
    java.security.Security.removeProvider(provider.getName());
    java.security.Security.insertProviderAt(provider, 2);
    com.safenetinc.luna.LunaSlotManager.getInstance().logout();
} catch (Exception e) {
    System.out.println("Exception caught during loading of the providers: "
        + e.getMessage());
}
```

Post-Installation Tasks

Making Private and Secret Keys Extractable

By default, all generated private and secret keys have their CKA_EXTRACTABLE attribute set to **0** (see ["Key Attribute Defaults" on page 338](#)). These keys are stored in the HSM hardware and cannot be extracted, only cloned to a partition on another HSM. This attribute cannot be modified later. If you want the ability to wrap private and/or secret keys and export them off the HSM, you must use one of the following two methods to set CKA_EXTRACTABLE to **1** (TRUE) when the key is created:

Global configuration:

Configure **java.security** as follows to have JSP create all future private/secret keys with CKA_EXTRACTABLE=1:

- > To make all private keys extractable, add the following line to **java.security**:
com.safenetinc.luna.provider.createExtractablePrivateKeys=true
- > To make all secret keys extractable, add the following line to **java.security**:
com.safenetinc.luna.provider.createExtractableSecretKeys=true

Local configuration:

Configure CKA_EXTRACTABLE on a key-by-key basis by using the following methods in your Java application:

- > To make the next generated private key extractable using the **LunaSlotManager.setPrivateKeysExtractable()** method:

```
LunaSlotManager.getInstance().setPrivateKeysExtractable(true); // Set CKA_EXTRACTABLE=1 on
upcoming private keys
kpg = KeyPairGenerator.getInstance("RSA", "LunaProvider");
kpg.initialize(2048);
myPair = kpg.generateKeyPair();
LunaSlotManager.getInstance().setPrivateKeysExtractable(false); // Set CKA_EXTRACTABLE=0 on
upcoming private keys
```

NOTE To wrap and export private keys, the partition must have partition policy 1: Allow private key wrapping set to 1 (ON). See [Configuring the Partition for Cloning or Export of Private Keys](#) in the *Administration Guide*.

- > To make the next generated secret key extractable using the **LunaSlotManager.setSecretKeysExtractable()** method:

```
LunaSlotManager.getInstance().setSecretKeysExtractable(true); // Set CKA_EXTRACTABLE=1 on
upcoming secret keys
kg = KeyGenerator.getInstance("AES");
kg.init(256);
aesKey = kg.generateKey();
LunaSlotManager.getInstance().setPrivateKeysExtractable(false); // Set CKA_EXTRACTABLE=0 on
upcoming secret keys
```

Using ECC Keys for TLS with Java 7

For optimal Java performance when using Elliptic Curve keys to perform TLS with Java 7, where those keys reside in the HSM, you must configure the SunEC security provider (sun.security.ec.SunEC) to be below the LunaProvider in your java.security file.

We suggest that you not attempt to resolve a performance issue by having the LunaProvider as the default because that would result in the symmetric keys also being used in the HSM which is not optimal for performance.

Managing Security for Java Developers

The SafeNet JSP is a Java API that is intended to be used as an interface between customer-written or third-party Java applications and the SafeNet Luna PCIe HSM. Managing security issues associated with the overall operational environment in which the application is running, including the user interface, is the responsibility of the application.

A common example would be input and capture of user name and password. The application, or a set of organizational procedures, is responsible for making the access control decision regarding whether the user has the necessary permissions (at the organizational level) to access the HSM's services and then must provide protection for the password as it is entered, and erasure from memory after the operation is completed. The SafeNet JSP will control access to the HSM based on the correct password being input from the application via the Login method, but security outside the HSM is your responsibility.

Non-standard ECDSA Mapping

The SafeNet provider maps the "ECDSA" signature algorithm to "NONEwithECDSA". The Java convention is to map it to "SHA1withECDSA". This is noted here in case you wish to use it in provider inter-operability testing. This mapping is noted in the Javadoc as well.

For comparison, "RSA" maps to "NONEwithRSA" while "DSA" maps to "SHA1withDSA".

Notes about thread safe, session safe, and multi-threading

PKCS#11 (the standard, and Gemalto's implementation) requires that a session can be used only by a single thread at a time. That is, multiple threads cannot access the same session simultaneously. Threads can share a session; however the application must ensure that only one thread accesses the session at a time. It is simpler for an application to assign a unique session for each thread, but applications do not need to follow that pattern.

Our LunaProvider endeavors to be thread safe in the way it uses our PKCS#11 library. But customer Java applications must follow the threading model defined by Java. For example, Java Cipher objects (essentially all crypto-related objects) are not thread safe according to the JSP specification. Similar to PKCS#11 sessions, only one thread should use a cipher object at a time. Our LunaProvider requires that the Java application follows that JSP approach.

Therefore, it is very possible, and expected, to see sessions being used by multiple threads, all in legitimate and thread-safe ways according to both JSP and PKCS#11.

SafeNet JSP Configuration

SafeNet JSP consists of a single JCA/JCE service provider, that allows a Java-based application to use SafeNet Luna PCIe HSM products for secure cryptographic operations. Please refer to the Javadocs accompanying the toolkit, for the most current information regarding the SafeNet JSP packages and LunaProvider functionality.

To install JSP, refer to ["SafeNet JSP Overview and Installation" on page 370](#).

SafeNet Java Security Provider

In general, you should use the standard JCA/JCE classes and methods to work with SafeNet Luna PCIe HSM. The following sections provide examples of when you may wish to use the special SafeNet methods.

Class Hierarchy

All public classes in the SafeNet Java crypto provider are included in the `com.safenetinc.luna` package or subpackages of that package. Thus the full class names are (for example):

- > `com.safenetinc.luna.LunaSlotManager`
- > `com.safenetinc.luna.provider.key.LunaKey`

If your application is compliant with the JCA/JCE spec, you will generally not need to directly reference any SafeNet implementation classes. Use the interfaces defined in the `java.security` packages instead. The exception is if you need to perform an HSM-specific operation, such as modifying PKCS#11 attributes.

Throughout the rest of this document, the short form of the class names is used for convenience and readability. The full class names (of SafeNet or other classes) are used only where necessary to resolve ambiguity.

Special Classes/Methods

The JCA/JCE interfaces were not designed with hardware security modules (HSMs) in mind and do not include methods for managing aspects of a hardware module. SafeNet JSP provides some additional functions in addition to the standard JCA/JCE API.

The `LunaSlotManager` class provides custom methods that allow some HSM-specific information to be retrieved. It also provides a way to log in to the HSM if your application cannot make use of the standard `KeyStore` interface. For details please check the Javadoc which comes with the product.

It is not always necessary to use the `LunaSlotManager` class. With proper use of the JCE API provided in SafeNet JSP, your code can be completely hardware-agnostic.

The `LunaKey` class implements the `Key` interface and provides all of the methods of that class along with custom methods for manipulating key objects on SafeNet hardware.

NOTE Sensitive attributes cannot be retrieved from keys stored on SafeNet hardware. Thus certain JCE-specified methods (such as `PrivateKeyRSA.getPrivateExponent()`) will throw an exception.

The `LunaCertificateX509` class implements the `X509Certificate` methods along with custom methods for manipulating certificate objects on SafeNet hardware.

Examples

The SafeNet JSP comes with several sample applications that show you how to use the Luna provider. The samples include detailed comments.

To compile on Windows without an IDE (Administrator privileges may be required):

```
cd <SafeNet Luna PCIe HSM install>/jsp/samples
javac com\safenetinc\luna\sample\*.java
```

To run:

```
java com.safenetinc.luna.sample.KeyStoreLunaDemo (or any other sample class in that package)
```

NOTE The Luna Keystore is not a physical file like a regular JKS. It is a virtual interface to the HSM and contains only handles for the private key objects.

Authenticating to the HSM

In order to make use of an HSM, it is necessary to activate the device through a login. Depending on the security level of the device, the login will require a plain-text password and/or a PED key.

The preferred method of logging in to the module is through the Java KeyStore interface. The store type is “Luna” and the password for the key store is the challenge for the partition specified.

KeyStore files for the Luna KeyStore must be created manually. The content of the KeyStore file differs if you wish to reference the partition by the slot number or label (preferred). Details of authenticating to the HSM via the KeyStore interface are explained in the Javadoc for LunaKeyStore and in the KeyStoreLunaDemo sample application.

NOTE We strongly recommend that you *use the application partition's label* as the identifier for the cryptographic slot on the HSM. That designator never changes, unless you explicitly change label. The slot number, on the other hand, might change, and therefore should not be used in your code.

Keys in a Luna KeyStore cannot have individual passwords. Only the KeyStore password is used. If your HSM requires PED keys to be presented for authentication and the partition is not already activated, loading the KeyStore will cause the PED to prompt you to present this key.

Other than the KeyStore interface your application may also make use of the LunaSlotManager class or by using a login state created outside of the application through a utility called ‘salogin’. Use of salogin is strongly discouraged unless you have a very specific need.

LunaKeyStoreMP is Deprecated

LunaKeyStoreMP is deprecated for SafeNet JSP, and may be discontinued in a future release.

LunaKeyStoreMP was used in previous releases to allow logical partitioning of the key space on HSMs that have only one partition. This allowed you to create a separate MP key store for each individual client that accessed the partition. Recent SafeNet releases, however, support multiple partitions, and dedicating a partition per client is a superior solution for management and security reasons.

NOTE LunaKeyStoreMP is retained for backwards compatibility reasons only. Do not use LunaKeyStoreMP when creating new applications.

Logging Out

Logging out of the HSM is performed implicitly when the application is terminated normally. Logging out of the HSM while the application is running can be done with the LunaSlotManager class. Please note that any ephemeral (non-persistent) key material present on the HSM will be destroyed when the session is logged out. Because the link to the HSM will be severed, cryptographic objects that were created by the LunaProvider will no longer be usable. Attempting to use these objects after logging out will result in undefined behavior.

All key material which was persisted on the HSM (either through the KeyStore interface or using the proprietary Make Persistent method) will remain on the HSM after a logout and will be accessible again when the application logs back in to the HSM.

Keytool

The SafeNet JSP may be used in combination with Java's keytool utility to store and use keys on a SafeNet Luna PCIe HSM, see ["Using Java Keytool with SafeNet Luna PCIe HSM" on page 389](#).

Cleaning Up

Keys that are made persistent will continue to exist on the HSM until they are explicitly destroyed, or until the HSM is reinitialized. Persistent keys that are no longer needed can be explicitly destroyed to free resources on the HSM.

Keys may be removed using the Keytool, or programmatically through the KeyStore interface or other methods available through the API.

LunaSlotManager contains methods that report the number of objects that exist on the HSM. See the Javadoc for LunaSlotManager for more information.

PKCS#11/JCA Interaction

Keys created using the SafeNet PKCS#11 API can be used with the SafeNet JSP; the inverse is also true.

Certificate Chains

The PKCS#11 standard does not provide a certificate chain representation. When a Java certificate chain is stored on a SafeNet token, the certificates of the chain appear as individual objects when viewed through the PKCS#11 API. In order for the LunaProvider to properly identify PKCS#11-created certificates as part of a chain attached to a private key, the certificates must follow the labeling scheme described below.

Java Aliases and PKCS#11 Labels

The PKCS#11 standard defines a large set of object attributes, including the object label. This label is analogous to the Object alias in a java KeyStore.

The SafeNet KeyStore key entry or a SafeNet KeyStore certificate entry will have a PKCS#11 object label exactly equal to the Java alias. Similarly, a key created through PKCS#11 will have a Java alias equal to the PKCS#11 label.

Because a java certificate chain cannot be represented as a single PKCS#11 object, the individual certificates in the chain will each appear as individual PKCS#11 objects. The labels of these PKCS#11 objects will be composed of the alias of the corresponding key entry, concatenated with "--certX", where 'X' is the index of the certificate in the java certificate chain.

For example, consider a token that has a number of objects created through the Java API. The objects consist of the following:

- > A key entry with alias "signing key", consisting of a private key and a certificate chain of length 2
- > A trusted certificate entry with alias "root cert"
- > A secret key with alias "session key"

If all objects on the token were viewed through a PKCS#11 interface, 5 objects would be seen:

- > A private key with label "signing key"
- > A certificate with label "signing key--cert0"
- > A certificate with label "signing key--cert1"

- > A certificate with label "root cert"
- > A secret key with label "session key"

NOTE PKCS#11 labels (strings of ascii characters) and Java aliases (of the `java.lang.String` type) are usually fully compatible, but problems can arise if non-printable characters are used. To maintain compatibility between Java and PKCS#11, avoid embedding non-printable or non-ascii characters in aliases or object labels.

RSA Cipher

Previously, by default, the SafeNet JSP RSA cipher mode used raw RSA X.509 encryption, with no padding.

For improved security and compatibility, default padding for RSA cipher has been changed from NoPadding to PKCS1v1_5.

The JC PROV PKCS#11 Java Wrapper

This section describes how to install and use the JC PROV Java wrapper for the PKCS#11 API. It contains the following topics:

- > ["JC PROV Overview" below](#)
- > ["Installing JC PROV" on the next page](#)
- > ["JC PROV Sample Programs" on the next page](#)
- > ["JC PROV Sample Classes" on page 381](#)
- > ["JC PROV API Documentation" on page 385](#)

JC PROV Overview

JC PROV is a Java wrapper for the PKCS#11 API. JC PROV is designed to be as similar to the PKCS#11 API as the Java language allows, allowing developers who are familiar with the PKCS#11 API to rapidly develop Java-based programs that exercise the PKCS#11 API.

AES-GMAC and AES-GCM are supported in JC PROV. Use `CK_AES_CMAC_PARAMS.java` to define the GMAC operation. Implementation is the same as for PKCS#11.

JDK compatibility

The JC PROV Java API is compatible with JDK 1.5.0 or higher.

The JC PROV library

The JC PROV library is implemented in `jcprov.jar`, under the namespace `com.safenetinc.jcprov`. It is accompanied by a shared library that provides the native methods used to access the appropriate PKCS#11 library. The name of the shared library is platform dependent, as follows:

Operating system	Shared library
Windows (64 bit)	jcprov.dll

Operating system	Shared library
Linux	libjcpov.so
Solaris	libjcpov.so
AIX	libjcpov.so

Installing JC PROV

Use the SafeNet Luna HSM Client Installer to install the JC PROV software (runtime and SDK packages). The software is installed in the location specified in the following table:

Operating system	Installation location
Windows	C:\Program Files\safenet\lunaclient\jcpov
Linux	/usr/safenet/lunaclient/jcpov
Solaris	/opt/safenet/lunaclient/jcpov
AIX	/usr/safenet/lunaclient/jcpov

The installation includes a **samples** subdirectory and a **javadocs** subdirectory.

Changing the Java JNI libraries (AIX only)

The Java VM on AIX does not support mixed mode JNI libraries. Mixed mode libraries are shared libraries that provide both 32-bit and 64-bit interfaces. It is therefore essential that you select the correct JNI library to use with your Java VM.

To configure the JNI library for use with a 64-bit Java VM:

1. Ensure that the `/usr/safenet/lunaclient/jcpov/lib/libjcpov.a` symbolic link points to a 64-bit version of the library (`libjcpov_64.a`), for example `/usr/safenet/lunaclient/jcpov/lib/libjcpov_64.a`.
2. Ensure that the `/usr/safenet/lunaclient/jcpov/lib/libcryptoki.a` symbolic link points to a 64-bit version of the library (`libcryptoki_64.a`), for example `/usr/safenet/lunaclient/jcpov/lib/libcryptoki_64.a`.

JC PROV Sample Programs

Several sample programs are included to help you become familiar with JC PROV. The binaries for the sample programs are included in the `jcprovsamples.jar` file. You must compile the binaries before you can use the sources provided.

Compiling and running the JC PROV sample programs

CAUTION! You require JDK 1.5.0 or newer to compile the JC PROV sample programs.

It is recommended that you compile the samples in their installed locations, so that the path leading to the samples directory in the installation location will allow them to be executed as documented below.

Prerequisites

For best results, perform the following actions before attempting to compile the sample programs:

- > Add **jcprov.jar** to your **CLASSPATH** environment variable
- > Add a path to the **CLASSPATH** environment variable that allows JC PROV to use the **com.safenetinc.jcprov.sample** namespace. This is required since all of the applications are registered under this namespace.

To compile the JC PROV sample programs on UNIX/Linux:

1. Set the **CLASSPATH** environment variable to point to **jcprov.jar** and the root path for the sample programs.
export CLASSPATH=<jcprov_installation_directory>/*
2. Change directory to the sample programs path.
cd /usr/safenet/lunaclient/jcprov/samples/com/safenetinc/jcprov/sample
3. Use the **javac** program to compile the examples.
javac GetInfo.java
4. Use the **java** program to run the samples.
java com.safenetinc.jcprov.sample.GetInfo -slot 0 -info

To compile the JC PROV sample programs on Windows:

1. Set the **CLASSPATH** environment variable to point to **jcprov.jar** and the root path for the sample programs:
C:\> set "CLASSPATH= C:\Program Files\safenet\lunaclient\jcprov\jcprov.jar; C:\program files\safenet\jcprov\samples"
2. Use the **javac** program to compile the examples:
C:\Program Files\safenet\lunaclient\jcprov\samples> javac GetInfo.java
3. Use the **java** program to run the samples:
C:\Program Files\safenet\lunaclient\jcprov\samples> java com.safenetinc.jcprov.sample.GetInfo -info -slot 0

JC PROV Sample Classes

JC PROV provides sample classes in the <jcprov_installation_directory>/**samples** directory. These include:

- > ["DeleteKey" on the next page](#)
- > ["EncDec" on the next page](#)
- > ["GenerateKey" on page 383](#)
- > ["GetInfo" on page 384](#)
- > ["Threading" on page 384](#)

Other samples contained in the **samples** directory may be more or less useful to you depending on what you need. Each relevant sample has a description of both its purpose and its parameters in the header section of its file.

DeleteKey

Demonstrates the deletion of keys.

A generated key is required to use this script. To generate a key, use ["GenerateKey" on the next page](#) or refer to ["Using Java Keytool with SafeNet Luna PCIe HSM" on page 389](#)

Usage

```
java com.safenetinc.jcprov.sample.DeleteKey -keyType <keytype> -keyName <keyname> [-slot <slotId>] [-password <password>]
```

Parameters

Parameter	Description
-keytype	Specifies the type of key you want to delete. Enter this parameter followed by one of the following supported key types: <ul style="list-style-type: none"> > des - single DES key > des2 - double-length, triple-DES key > des3 - triple-length, triple-DES key > rsa - RSA key pair
-keyName	Specifies the name (label) of the key you want to delete. Enter this parameter followed by the name (label) of the key you want to delete.
-slot	Specifies the slot for the HSM or partition that contains the key you want to delete. Optionally enter this parameter followed by the slot identifier for the HSM or partition that contains the key you want to delete. If this parameter is not specified, the default slot is used. Default: 1
-password	Specifies the password for the slot. Optionally enter this parameter followed by the slot password to delete a private key.

EncDec

Demonstrates encryption and decryption operations by encrypting and decrypting a string.

A generated key is required to use this script. To generate a key, use ["GenerateKey" on the next page](#) or refer to ["Using Java Keytool with SafeNet Luna PCIe HSM" on page 389](#)

Usage

```
java com.safenetinc.jcprov.sample.EncDec -keyType <keytype> -keyName <keyname> [-slot <slotId>] [-password <password>]
```

Parameters

Parameter	Description
-keytype	Specifies the type of key you want to use to perform the encryption/decryption operation. Enter this parameter followed by one of the following supported key types: <ul style="list-style-type: none"> > des - single DES key > des2 - double-length, triple-DES key > des3 - triple-length, triple-DES key > rsa - RSA key pair
-keyName	Specifies the name (label) of the key you want to use to perform the encryption/decryption operation. Enter this parameter followed by the name (label) of the key you want to use to perform the encryption/decryption operation.
-slot	Specifies the slot for the HSM or partition that contains the key you want to use to perform the encryption/decryption operation. Optionally enter this parameter followed by the slot identifier for the HSM or partition that contains the key you want to use to perform the encryption/decryption operation. If this parameter is not specified, the default slot is used. Default: 1
-password	Specifies the password for the slot. Optionally enter this parameter followed by the slot password to encrypt/decrypt a private key.

GenerateKey

Demonstrates the generation of keys.

Usage

```
java com.safenetinc.jcprov.sample.GenerateKey -keyType <keytype> -keyName <keyname> [-slot <slotId>] [-password <password>]
```

Parameters

Parameter	Description
-keytype	Specifies the type of key you want to generate. Enter this parameter followed by one of the following supported key types: <ul style="list-style-type: none"> > des - single DES key > des2 - double-length, triple-DES key > des3 - triple-length, triple-DES key > rsa - RSA key pair
-keyName	Specifies the name (label) of the key you want to generate. Enter this parameter followed by the name (label) of the key you want to generate.

Parameter	Description
-slot	Specifies the slot for the HSM or partition where you want to generate the key. Optionally enter this parameter followed by the slot identifier for the HSM or partition where you want to generate the key. If this parameter is not specified, the default slot is used. Default: 1
-password	Specifies the password for the slot. Optionally enter this parameter followed by the slot password to generate a private key.

GetInfo

Demonstrates the retrieval of slot and token information.

Usage

```
java com.safenetinc.jcprov.sample.GetInfo {-info | -slot [<slotId>] | -token [<slotId>]}
```

Parameters

Parameter	Description
-info	Retrieve general information.
-slot	Retrieve slot information for the specified slot. Enter this parameter followed by the slot identifier for the slot you want to retrieve information from. If <slotId> is not specified, information is retrieved for all available slots.
-token	Retrieve token information for the HSM or partition in the specified slot. Enter this parameter followed by the slot identifier for the HSM or partition you want to retrieve information from. If <slotId> is not specified, information is retrieved for all available slots.

Threading

This sample program demonstrates different ways to handle multi-threading.

This program initializes the Cryptoki library according to the specified locking model. Then a shared handle to the specified key is created. The specified number of threads is started, where each thread opens a session and then enters a loop which does a triple DES encryption operation using the shared key handle.

It is assumed that the key exists in slot 1, and is a Public Token object.

A generated key is required to use this script. To generate a key, use ["GenerateKey" on the previous page](#) or refer to ["Using Java Keytool with SafeNet Luna PCIe HSM" on page 389](#)

Usage

```
java com.safenetinc.jcprov.sample.Threading -numThreads <numthreads> -keyName <keyname> -locking { none | os | functions } [-v]
```

Parameters

Parameter	Description
-numthreads	Specifies the number of threads you want to start. Enter this parameter followed by an integer that specifies the number of threads you want to start.
-keyName	Specifies the triple-DES key to use for the encryption operation. Enter this parameter followed by the name (label) of the key to use for the encryption operation.
-locking	Specifies the locking model used when initializing the Cryptoki library. Enter this parameter followed by one of the following locking models: <ul style="list-style-type: none"> > none - do not use locking when initializing the Cryptoki library. If you choose this option, some threads should report failures. > os - use the native operating system mechanisms to perform locking. > functions - use Java functions to perform locking
-v	Specifies the password for the slot. Optionally enter this parameter followed by the slot password to generate a private key.

JCPROV API Documentation

The JCPROV API is documented in a series of javadocs. The documentation is located in the `<jcprov_installation_directory>/javadocs` directory.

Java or JSP Errors

In the process of using our JSP (Java Service Provider) or programming for Java clients, you might encounter a variety of errors generated by various levels of the system. In rare cases those might be actual problems with the system, but in the vast majority of cases the errors are the system (or the Client-side libraries) telling you that you (or your application) have done something "wrong". In other words, the error messages are guidance to ensure that your actions and your programs are giving the system what it needs (in the right order and format) to complete the tasks that you ask of it.

Keep in mind that there are several levels involved. The SafeNet appliance and its HSM keycard have both software and firmware built in. Among other things, the system software handles the system side of communication between you (either as administrator or as Client) and the HSM on the appliance. In general, a client-side program (or programmer) would not encounter error messages directly from the system. If an error condition arises on the system, the most likely visibility would be error messages in the system logs - viewed by the appliance administrator - or else client-side messages based upon the interaction of the client-side software (ours and yours) with the appliance.

On the client side, the JSP and any Java programs that you use would be overlaid on, and using, the SafeNet library, which is an extended version of PKCS#11, customized to make use of our HSM (the standard itself and the cryptoki library are oriented toward in-software implementation of cryptographic functions, with some generic support of generic HSM functions, leaving room for each HSM supplier to support their own special

functions by extending the standard). PKCS#11 is an RSA Laboratories cryptographic standard, and our libraries are a C-language implementation of that standard. You can view all that is known about PKCS#11 error conditions and messages at the [RSA website](#).

See "[Library Codes](#)" on [page 1](#) for a summary of error codes and their meanings, which includes the SafeNet extensions to the PKCS#11 standard that are specific to our HSM. Note that "error codes" do not usually indicate a problem with the appliance or HSM - they indicate an exception condition has been encountered, possibly because you (or your application) stopped/canceled a requested action before it could complete, provided incorrect or incomplete or wrongly-formatted input data, and so on, or possibly because a network connection has been disrupted, power has failed, or any of a variety of situations has been detected.

The JSP and your Java programming are overlaid on top of the PKCS#11 and SafeNet libraries. An error reported by a Java application might refer to a problem at the Java or JSP level, or the error might have been passed through from a lower level.

If you receive a cryptic error that looks something like:

```
Exception in thread "main"
```

```
com.safenetinc.crypto.LunaCryptokiException: function 'C_Initialize' returns 0x30
```

then this error has been passed through from a lower layer and is not a Java or JSP error. You should look in the Error Codes page (link above) or in the PKCS#11 standard for the meaning of any error in a similar format.

In general, we wrap cryptoki exception codes. Most exceptions thrown by the JSP are in accordance with the specification. Check the Javadoc for the API call that threw the exception.

- > LunaException is used to report a LunaProvider-specific exception.
- > LunaCryptokiException reports errors returned by the HSM. Those might be wrapped in other Exceptions.

Re-Establishing a Connection Between Your Java Application and SafeNet Luna PCIe HSM

Thales Group provides Java code samples for performing various application functions. For the proper method for performing a reconnect between a Java application and the SafeNet Luna PCIe HSM in the event of a disconnect, see **MiscReconnectDemo.java** in the Samples folder.

Recovering From the Loss of All HA Members

The `reinitialize` method of the **LunaSlotManager** class takes the role of the PKCS#11 functions **C_Finalize** and **C_Initialize**. It is intended to be used when a complete loss of communication happens with all the members of your High Availability (HA) group.

This section describes the situations in which you should use this method, the effect this method has on a running application, and how to use this method safely. It is assumed that the auto-recovery features of the HA group are enabled.

You should read this section if you are developing an application that uses the LunaProvider in an environment that leverages an HA group of SafeNet Luna PCIe HSM appliances, so that you can safely recover an entire HA group.

When to Use the reinitialize Method

When using the high-availability (HA) features of SafeNet Luna PCIe HSM, the auto-recovery feature will resolve situations where connectivity is lost to a subset of members for a brief time. However, if you lose connection to all members then the connection cannot be automatically recovered. Finalizing the library and initializing it again is the only way to recover other than restarting the application.

Why the Method Must Be Used

In an HA group, we rely on having at least one member present in order to maintain state. If all of the members have been lost, then we cannot make any determination of which member has a known good state. Also, when a connection to a member is lost, the authenticated state is lost. When an individual member returns, we can use the authenticated state from another member to authenticate to the one that has returned. When all members are lost, then the authenticated state is lost on all members.

What Happens on the HSM

The Network Trust Link Service (NTLS) on the HSM appliance is responsible for cleaning up any cryptographic resources, such as session objects, and cryptographic operation contexts when a connection to the client is lost. This happens when the socket closes.

Effect on Running Applications

All resources created within the LunaProvider must be treated as junk after the library is finalized. Sessions will no longer be valid, session objects will point to non-existent objects or worse to a wrong object, and

Signature/Cipher/Mac/etc objects will have invalid data.

Even **LunaKey** objects, which represent persistent objects, may contain invalid data. When the virtual slot is constructed in the library, the virtual object table is built from the objects present on each individual member. There is no guarantee that objects will have the same handle from one initialization to the next. This is true from the moment the connection to the group is severed. All these resources must be released before calling the reinitialize method. Beyond causing undesirable behavior when used, if these objects are garbage collected after cryptographic operations resume, they can result in the deletion of new objects or sessions.

Using the Method Safely

The first indication that all communications may have been lost with the group is a **LunaException** reporting an error code of **0x30** (Device Error). Other possible error codes that can indicate this status are **0xE0** (Token not present) and **0xB3** (Session Handle invalid). The **LunaException** class does not provide the error code as a discrete value and you will have to parse the message string to determine this value.

At this point, you should validate that the group has been lost. The **com.safenetinc.luna.LunaHAStatus** object is best suited for this. Your application should know the slot number of the HA slot that you are using because it may not be able to query this information from the label when the slot is missing.

Example

```
LunaHAStatus status = new LunaHAStatus(haSlotNumber);
```

You can query the object for detailed information or just use the **isOK()** method to determine if the group has been lost. The **isOK()** method will return true if all members are still present. If all members are gone, an exception will be thrown.

If no application is thrown, the application should be able to proceed operating, and any individual members of the HA group that have been lost will be recovered by the library. Further details on failed members can be queried through the `LunaHASStatus` object.

In many highly threaded applications, such as web applications, it is desirable to have a singleton, which is responsible for keeping track of the health of the HSM connection. This can be done by having worker threads report information to this singleton, by having a specific health check thread, or through a combination of the two.

Once the error state is discovered, all worker threads should be stopped or allowed to return an error. It may take up to 40 seconds from the time the group was lost for all threads to discover that there is an error. It can take 20 seconds for any given command to time out as a result of network failure. Once this happens, new commands will not be sent to that HSM, but a command may have just been sent and that command will have its own 20-second timeout. As mentioned above, in the section on application effects, all of the objects created or managed by the `LunaProvider` must be considered at this point to contain junk data. Operating after recovery with this junk data can cause undesired effects. This means all keys, signature, cipher, Mac, `KeyGenerator`, `KeyPairGenerator`, `X509Certificate`, and similar objects must be released to the garbage collector. Instances of most non-SPI (`LunaAPI`, `LunaSlotManager`, `LunaTokenManager`, etc.) objects do not pose a problem, but any instances of `LunaSession` held in the application during the course of the reinitialize can cause problems if they are returned to the session pool after the reinitialization takes place.

Cryptographic processing in the application should be halted until connection with the HSMs is back to a known good state. It may be appropriate to hold operations in a queue for processing later or to return an Out of Service message.

Once the objects have been released and no further processing will occur, the application should attempt recovery of the connection. This is done through the `com.safenetinc.luna.LunaSlotManager.reinitialize` method. This method will first clear session objects held within the provider before finalizing the library. After the library is finalized, it will initialize it again by invoking the `C_Initialize` method. This method will establish a connection with all the HSMs if possible. The same `isOK()` method of `LunaHASStatus` can be used to determine if the group has been recovered successfully.

It is also important to only have a single thread call the `reinitialize` method. When multiple threads try to unload or load the library at the same time, errors can occur.

Using Java Keytool with SafeNet Luna PCIe HSM

This page describes how to use the Java KeyTool application with the LunaProvider.

Limitations

The following limitations apply:

- > You cannot use the `importkeystore` command to migrate keys from a Luna KeyStore to another KeyStore.
- > Private keys cannot be extracted from the KeyStore unless you have the Key Export model of the HSM.
- > By default secret keys created with the LunaProvider are non-extractable.

The example below uses a KeyStore file containing only the line “slot:0”. This tells the Luna KeyStore to use the token in slot 0.

NOTE The Luna Keystore is not a physical file like a regular JKS. It is a virtual interface to the HSM and contains only handles for the private key objects.

For information on creating keys through Key Generator or Key Factory classes please see the LunaProvider Javadoc or the JCA/JCE API documentation.

Keys (with self signed certificates) can be generated using the keytool by specifying a valid Luna KeyStore file and specifying the KeyStore type as “Luna”. The password presented to authenticate to the KeyStore is the challenge password of the partition.

Example

```
keytool -genkeypair -alias myKey -keyalg RSA -sigalg SHA256withRSA -keystore keystore.luna -
storetype Luna
Enter keystore password:
What is your first and last name?
[Unknown]: test
What is the name of your organizational unit?
[Unknown]: codesigning
What is the name of your organization?
[Unknown]: SafeNet Inc
What is the name of your City or Locality?
[Unknown]: Ottawa
What is the name of your State or Province?
[Unknown]: ON
What is the two-letter country code for this unit?
[Unknown]: CA
Is CN=test, OU=codesigning, O=SafeNet Inc, L=Ottawa, ST=ON, C=CA correct?
[no]: yes
Enter key password for <myKey>
(RETURN if same as keystore password):
```

Keytool Usage and Examples

The LunaProvider is unable to determine which PKCS#11 slot to use without providing a keystore file. This file can be manually created to specify the desired slot by either the slot number or partition label. The naming of the files is not important - only the contents.

The keytool examples below refer to a keystore file named bylabel.keystore. Its content is just one line:

```
tokenlabel:a-partition-name
```

where a-partition-name is the name of the partition you want the Java client to use.

Here is the (one line) content of a keystore file that specifies the partition by slot number:

```
slot:0
```

where 1 is the slot number of the partition you want the Java client to use.

To test that the Java configuration is correct, execute:

```
my-lunaclient:~/luna-keystores$ keytool -list -v -storetype Luna -keystore bylabel.keystore
```

The system requests the password of the partition and shows its contents.

Here is a sample command to create an RSA 2048 bit key with SHA256withRSA self-signed certificate. This example uses java 6, other versions might be slightly different.

```
keytool -genkeypair -alias keyLabel -keyalg RSA -keysize 2048 -sigalg SHA256withRSA -storetype Luna -keystore bylabel.keystore -validity 365
```

```
Enter keystore password:
```

```
What is your first and last name?
```

```
[Unknown]: mike
```

```
What is the name of your organizational unit?
```

```
[Unknown]: appseng
```

```
What is the name of your organization?
```

```
[Unknown]: safenet
```

```
What is the name of your City or Locality?
```

```
[Unknown]: ottawa
```

```
What is the name of your State or Province?
```

```
[Unknown]: on
```

```
What is the two-letter country code for this unit?
```

```
[Unknown]: ca
```

```
Is CN=mike, OU=appseng, O=safenet, L=ottawa, ST=on, C=ca correct?
```

```
[no]: yes
```

```
Enter key password for <keyLabel>
```

```
(RETURN if same as keystore password):
```

With the Luna provider there is no concept of a key password and anything entered is ignored.

The following is a more elaborate sequence of keytool usage where the final goal is to have the private key generated in the HSM through keytool “linked” to its certificate.

Import CA certificate

It is mandatory to import the CA certificate – keytool verifies the chain before importing a client certificate:

```
my-lunaclient:~/luna-keystores$ keytool -importcert -storetype Luna -keystore bylabel.keystore -alias root-mikeca -file mike_CA.crt
```

It is not required to import this certificate in the Java default cacerts keystore.

Generate private key

Generate the private key. It is not important that the `sigalg` specified matches the one used by the CA. You can also have `OU`, `O`, `L`, `ST`, and `C` different from the ones in the CA certificate.

```
my-lunaclient:~/luna-keystores$ keytool -genkeypair -alias java-client2-key -keyalg RSA -keysize
2048 -sigalg SHA256withRSA -storetype Luna -keystore bylabel.keystore
Enter keystore password:
What is your first and last name?
[Unknown]: java-client2
What is the name of your organizational unit?
[Unknown]: SE
What is the name of your organization?
[Unknown]: SFNT
What is the name of your City or Locality?
[Unknown]: bgy
What is the name of your State or Province?
[Unknown]: bg
What is the two-letter country code for this unit?
[Unknown]: IT
Is CN=java-client2, OU=SE, O=SFNT, L=bgy, ST=bg, C=IT correct?
[no]: yes
Enter key password for <java-client2-key>
(RETURN if same as keystore password):
```

Verify that the private key is in the partition:

```
my-lunaclient:~/luna-keystores$ keytool -list -v -storetype Luna -keystore bylabel.keystore
Enter keystore password:
Keystore type: LUNA
Keystore provider: LunaProvider
Your keystore contains 2 entries
Alias name: root-mikeca
Creation date: Oct 4, 2012
Entry type: trustedCertEntry
Owner: EMAILADDRESS=username@gemalto.com, CN=mike CA, OU=SE, O=SFNT, L=bgy, ST=bg, C=IT
Issuer: EMAILADDRESS=username@gemalto.com, CN=mike CA, OU=SE, O=SFNT, L=bgy, ST=bg, C=IT
Serial number: 1
Valid from: Thu Oct 04 09:02:00 CEST 2012 until: Tue Oct 04 09:02:00 CEST 2022
Certificate fingerprints:
    MD5: A2:15:4F:94:70:2B:D2:F7:C0:96:B1:47:F2:1D:03:E9
    SHA1: B3:4A:68:0A:8D:12:39:86:11:CE:EF:22:1B:D1:DE:8D:E9:19:2B:F4
    Signature algorithm name: SHA256withRSA
    Version: 3
*****
*****
Alias name: java-client2-key
Creation date: Oct 4, 2012
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=java-client2, OU=SE, O=SFNT, L=bgy, ST=bg, C=IT
Issuer: CN=java-client2, OU=SE, O=SFNT, L=bgy, ST=bg, C=IT
Serial number: 506d42dd
Valid from: Thu Oct 04 10:03:41 CEST 2012 until: Wed Jan 02 09:03:41 CET 2013
Certificate fingerprints:
    MD5: 7A:37:72:6B:8A:05:B6:49:91:70:0F:C4:04:1F:69:D9
    SHA1: 05:CD:9F:A5:37:0B:A6:A3:65:24:56:40:5E:29:2D:95:2D:53:8F:5F
    Signature algorithm name: SHA256withRSA
    Version: 3
```

Create the CSR

Create the CSR to be submitted to the CA.

```
my-lunaclient:~/luna-keystores$ keytool -certreq -alias java-client2-key -file client2-mikeca.csr
-storetype Luna -keystore bylabel.keystore
```

Enter keystore password:

Now have the CSR signed by the CA. Have the issued certificate exported to include the certificate chain.

Without the chain, keytool fails with the error:

```
java.lang.Exception: Failed to establish chain from reply
```

If you do not have the chain, you can use the steps in the section below to build the chain yourself.

To translate a PKCS#7 exported certificate from DER format to PEM format use the following:

```
my-lunaclient $ openssl pkcs7 -inform der -in Luna_Key.p7b -outform pem -out Luna_Key-pem.p7b
```

Microsoft CA exports certificates with chain only in PKCS#7 PEM encoded format.

Import client certificate

Now import the client certificate:

```
user@myserver:~/luna-keystores$ keytool -importcert -storetype Luna -keystore bylabel.keystore -
alias java-client2-key -file java-client2.crt
```

Enter keystore password:

Certificate reply was installed in keystore

Ensure that it is linked to the private key generated previously – the chain length is not 1 (Certificate chain length: 2)

```
user@myserver:~/luna-keystores$ keytool -list -v -storetype Luna -keystore bylabel.keystore
```

Enter keystore password:

Keystore type: LUNA

Keystore provider: LunaProvider

Your keystore contains 2 entries

Alias name: root-mikeca

Creation date: Oct 4, 2012

Entry type: trustedCertEntry

Owner: EMAILADDRESS=username@gemalto.com, CN=mike CA, OU=SE, O=SFNT, L=bggy, ST=bg, C=IT

Issuer: EMAILADDRESS=username@gemalto.com, CN=mike CA, OU=SE, O=SFNT, L=bggy, ST=bg, C=IT

Serial number: 1

Valid from: Thu Oct 04 09:02:00 CEST 2012 until: Tue Oct 04 09:02:00 CEST 2022

Certificate fingerprints:

MD5: A2:15:4F:94:70:2B:D2:F7:C0:96:B1:47:F2:1D:03:E9

SHA1: B3:4A:68:0A:8D:12:39:86:11:CE:EF:22:1B:D1:DE:8D:E9:19:2B:F4

Signature algorithm name: SHA256withRSA

Version: 3

Alias name: java-client2-key

Creation date: Oct 4, 2012

Entry type: PrivateKeyEntry

Certificate chain length: 2

Certificate[1]:

Owner: CN=java-client2, OU=SE, O=SFNT, L=bggy, ST=bg, C=IT

Issuer: EMAILADDRESS=username@gemalto.com, CN=mike CA, OU=SE, O=SFNT, L=bggy, ST=bg, C=IT

Serial number: 5

Valid from: Thu Oct 04 10:07:00 CEST 2012 until: Fri Oct 04 10:07:00 CEST 2013

Certificate fingerprints:

MD5: 4B:F0:9E:BC:EB:6A:88:2B:87:3A:76:35:7C:DE:4B:B4

SHA1: F1:0C:BC:E3:A1:97:E4:8B:24:2D:44:43:7A:EA:71:52:B3:C3:20:D7

Signature algorithm name: SHA256withRSA

```

Version: 3
Certificate[2]:
Owner: EMAILADDRESS=username@gemalto.com, CN=mike CA, OU=SE, O=SFNT, L=bgg, ST=bg, C=IT
Issuer: EMAILADDRESS=username@gemalto.com, CN=mike CA, OU=SE, O=SFNT, L=bgg, ST=bg, C=IT
Serial number: 1
Valid from: Thu Oct 04 09:02:00 CEST 2012 until: Tue Oct 04 09:02:00 CEST 2022
Certificate fingerprints:
    MD5:  A2:15:4F:94:70:2B:D2:F7:C0:96:B1:47:F2:1D:03:E9
    SHA1: B3:4A:68:0A:8D:12:39:86:11:CE:EF:22:1B:D1:DE:8D:E9:19:2B:F4
Signature algorithm name: SHA256withRSA
Version: 3

```

How to build a certificate with chain ...

When you receive the client certificate without the chain, it is possible to build a PKCS#7 certificate that includes the chain (and then feed it to `keytool -importcert`). In short, the “single” certificates without the chain can be “stacked” together by manually editing a PEM cert file; this PEM cert file can then be translated into a PKCS#7 cert. How? Like this:

1. Prerequisites. Have all the certs in .crt format. The cert in this format is represented as an ASCII file starting with the line

```
-----BEGIN CERTIFICATE-----
```

and ending with

```
-----END CERTIFICATE-----
```

For example, if the client cert is issued by a subCA and the subCA is signed by a root CA, you will have 3 cert files – the client cert, the subCA cert, and the root CA cert. If the certs are not in .crt format, `openssl` can be used to transform the format that you have into .crt format. See notes below.

2. Open a new text file, calling it, for example, `cert-with-chain.crt`. Insert into this file the content of the certificates in the chains. For the above example, you must first insert the client cert, then the subCA cert, then the root CA cert. The content of the file would then resemble the following:

```

-----BEGIN CERTIFICATE-----
    <-- client cert goes here
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    <-- subCA cert goes here
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    <-- root CA cert goes here
-----END CERTIFICATE-----

```

3. Use the following `openssl` command to convert the new certificate with chain, that you just created above, to a PKCS#7 certificate with chain:

```
my-sa $ openssl crl2pkcs7 -nocrl -certfile HSM_Luna-manual-chain.crt -out HSM_Luna-manual-chain.p7b -certfile root_CA.crt
```

4. Keytool is then able to import this .p7b certificate into the Luna keystore and correctly validate the chain.

Additional minor notes

1. Command to add a CA to the default CA cert store “cacerts”:

```
root@myserver:~# keytool -importcert -trustcacerts -alias root-mikeca -file /home/mike/luna-keystores/mike_CA.crt -keystore /etc/java-6-sun/security/cacerts
```

2. Use the following openssl command to convert a PKCS#7 certificate DER-encoded into a PKCS#7 PEM-encoded certificate:

```
user@myserver:~/tmp/$ openssl pkcs7 -inform der -in java-client2.p7b -out java-client2-pem.p7b
```

3. Use the following openssl command to convert a PKCS#7 DER-encoded certificate into a .crt PEM certificate:

```
user@myserver:~/tmp/$ openssl pkcs7 -print_certs -inform der -in mike_CA.p7b -out mike_CA-p7-2-crt.crt
```

4. Use the following openssl command to convert a PEM certificate with chain to a PKCS#7 with chain:

```
user@myserver:~/tmp/$ openssl crl2pkcs7 -nocrl -certfile HSM_Luna-manual-chain.crt -out HSM_Luna-manual-chain.p7b -certfile mike_CA.crt
```

CHAPTER 8: Microsoft Interfaces

This chapter describes the Microsoft interfaces to the PKCS#11 API. It contains the following topics:

- > ["SafeNet CSP Registration Utilities" below](#)
- > ["SafeNet KSP for CNG Registration Utilities" on page 399](#)
- > ["SafeNet CSP Calls and Functions" on page 404](#)

SafeNet CSP Registration Utilities

This section describes how to use the SafeNet CSP registration tool and related utilities to configure the Luna HSM client to use a SafeNet Luna PCIe HSM with Microsoft Certificate Services. You must be the client Administrator or a member of the Administrators group to run the SafeNet CSP tools.

The SafeNet CSP can be used by any application that acquires the context of the SafeNet CSP. All users who log in and use the applications that acquired the context have access to the SafeNet CSP. After you register the SafeNet Luna PCIe HSM partitions with SafeNet CSP, your CSP and KSP code should work the same whether the SafeNet Luna PCIe HSM (crypto provider) or the default provider is selected.

The SafeNet CSP is an optional client feature. During client installation, select **CSP (CAPI) / KSPCNG** to install it. To install the feature later, run the client installer again, select the option, and click **Modify**.

By default, the SafeNet CSP utilities are installed in `<client_install_dir>/CSP`. The installation includes **LunaCSP.dll**, the library used by CSP to interact with **Cryptoki.dll**, and the following utilities:

- > **"register" below**
 - ["Registering Partitions/HA Groups to CSP" on the next page](#)
 - ["Registering Cryptographic Algorithms to be Used in Software" on page 397](#)
 - ["Enabling Key Counting" on page 397](#)
- > **"ms2Luna" on page 397** — Used to migrate Microsoft CSP keys to a SafeNet Luna PCIe HSM partition
- > **"keymap" on page 398** — Used to manage keys on the partition for use with Microsoft CSP

register

You can use the CSP registration tool (`<client_install_dir>/CSP/register.exe`) to perform the following functions:

- > Register application partitions/HA groups and their passwords/challenge secrets for use with the SafeNet CSP (see ["Registering Partitions/HA Groups to CSP" on the next page](#)).
- > Register which non-RSA cryptographic algorithms you want performed in software only (see ["Registering Cryptographic Algorithms to be Used in Software" on page 397](#)).
- > Enable key counting in KSP/CSP (see ["Enabling Key Counting" on page 397](#)).
- > Register the provider library with the Windows OS to make it available for applications.

Syntax

register.exe [/partition | /algorithms | /library | /usagelimit] [/highavail] [/strongprotect] [/cryptouser] [/?]

Argument	Shortcut	Description
/algorithms	/a	Register algorithms that will be used in software by Microsoft CSP (i.e. not on the HSM). Only non-RSA algorithms can be configured to run in software; RSA algorithms will always run on the HSM hardware.
/cryptouser	/c	Register the password/challenge for the Crypto User (read-only crypto role). If this option is not specified, the Crypto Officer password/challenge is registered.
/highavail	/h	Register the virtual partition of a high-availability (HA) group.
/library	/l	Register the library and associated provider names for use with CSP. The following providers are registered: <ul style="list-style-type: none"> > Luna enhanced RSA and AES provider for Microsoft Windows > Luna Cryptographic Services for Microsoft Windows > Luna SChannel Cryptography Services for Microsoft Windows <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE This operation is deprecated; library registration is automatic.</p> </div>
/partition	/p	Register a partition and its password/challenge. You are prompted to select which available partitions to register to the CSP. This is the default option. If you type register with no additional parameters, then /partition is assumed. For example, register /strongprotect is the same as register /partition /strongprotect .
/strongprotect	/s	Strongly protect the challenge for registered partitions. This option ensures that only existing client users can access the CSP partitions. After running register /strongprotect , new users are not allowed to use CSP.
/usagelimit	/u	Set the maximum usage limit for RSA keys using CSP. Enter 0 to register unlimited uses.

Registering Partitions/HA Groups to CSP

Use the **"register" on the previous page** utility to register application partitions or HA virtual slots to the CSP. The Crypto Officer or Crypto User must complete this procedure, depending on which role you wish to use.

NOTE You cannot register a combination of HA groups and application partitions; either physical or virtual slots may be registered to the CSP at one time.

To register an application partition or HA group to the CSP

1. In a command prompt, navigate to the SafeNet CSP install directory and register the desired application partition(s) or HA group(s). Specify **/cryptouser** to register the CU role. Otherwise, the CO role will be registered. If you want to register both roles, you can run the command twice, once with **/cryptouser** and once without.

"register" on page 395 [/highavail] [/cryptouser]

You are prompted (y/n) to decide whether to register each available partition or HA virtual slot.

2. Install and/or configure your application(s).
3. Run each of your applications once to use SafeNet CSP.
4. Ensure the security of the registered role passwords/challenges by specifying **/strongprotect**.

"register" on page 395 /strongprotect

You can now run all applications as usual.

Registering Cryptographic Algorithms to be Used in Software

Certain symmetric operations such as hashing may be completed faster in software than on the SafeNet Luna PCIe HSM. The **register /algorithms** command allows you to choose which algorithms to de-register from the SafeNet Luna PCIe HSM. This may improve performance for operations that use these algorithms, but there is a security cost (exposing the operation in software). Signing and other asymmetric operations are always done on the HSM.

To register algorithms for software-only use

1. In a command prompt, navigate to the SafeNet CSP install directory and register the desired algorithms to be used in software.

"register" on page 395 /algorithms

You are prompted (y/n) to decide whether each available algorithm should be used in software.

Enabling Key Counting

Key counting allows you to specify the maximum number of times that a key can be used.

To enable key counting

1. In a command prompt, navigate to the SafeNet CSP install directory and register the key usage limit.

"register" on page 395 /usagelimit

You are prompted to enter a key usage limit. You can turn the feature off (unlimited uses) by entering **0**.

ms2Luna

Use the **ms2Luna** utility (<client_install_dir>/**CSP/ms2Luna.exe**) to migrate existing Microsoft CSP keys held in software to a registered partition/HA group on the SafeNet Luna PCIe HSM. It requires the thumbprint of a certificate held in the client's keystore.

Prerequisites

- > You must already have registered a partition/HA group using the **"register" on page 395** utility.
- > Private keys must be exportable to be migrated to the HSM.

To migrate Microsoft CSP keys to the SafeNet Luna PCIe HSM

1. In a command prompt, navigate to the SafeNet CSP install directory and migrate your existing keys to the HSM.

ms2Luna

You are prompted for the CSP certificate thumbprint.

keymap

Use the **keymap** utility (<client_install_dir>/**CSP/keymap.exe**) to manage keys for use with CSP. CSP needs three objects for a certificate to work:

- > Private key
- > Public key
- > A container: data object containing the certificate's association with the keys

A container is automatically created for all keypairs created using the CSP. For existing keypairs that were created outside the CSP, you must create a container and associate it with each keypair to make them available to the CSP.

When you run the **keymap** utility and select an available slot, the following options are available:

Option	Name	Description
1	Browse Objects	List the objects on the slot (public keys, private keys, and containers) that can be used by the CSP.
2	Create Key Container	Create a key container that can be used by the CSP.
3	View Key Container	Display information about a key container and the keys associated with it.
4	Associate Keys With Container	Map a keypair to an existing container. There are two possible algorithm mappings, depending on the intended purpose of the keypair: <ul style="list-style-type: none"> > Signature: keypair will be used for signing operations > Exchange: keypair will be used for key exchange
5	Do Nothing	Take no action.
99	Destroy Key Container	Destroy a key container object. This has no effect on the keys associated with a container.
0	Exit	Exit the keymap utility.

SafeNet KSP for CNG Registration Utilities

CNG (Cryptography Next Generation) is Microsoft's cryptographic application programming interface (API), replacing the older Windows cryptoAPI (CAPI). CNG adds new algorithms along with additional flexibility and functionality. Thales Group provides SafeNet CSP for applications running in older Windows crypto environments (running CAPI), and SafeNet KSP for newer Windows clients (running CNG). Consult Microsoft documentation to determine which one is appropriate for your client operating system.

KSP must be installed on any computer that is intended to act via CNG as a client of the HSM, running crypto operations in hardware. You need KSP to integrate SafeNet cryptoki with CNG and to use the newer functions and algorithms in Microsoft IIS.

After you register the SafeNet Luna PCIe HSM partitions with SafeNet KSP, your KSP code should work the same whether a SafeNet HSM (crypto provider) or the default provider is selected.

NOTE Be aware when working in a mixed environment or updating applications that previously used CAPI and the SafeNet CSP - the new algorithms supported by CNG (such as SHA512 and ECDSA) in Certificate Services are not recognized by systems that use CAPI. If Certificate Services is configured to use any of these new algorithms then the signed certificates can be installed only on systems that are aware of these new algorithms. Any of the systems that use CAPI will not be able to use this feature and certificate installation will fail.

The SafeNet KSP is an optional client feature. During client installation, select **CSP (CAPI) / KSPCNG** to install it. To install the feature later, run the client installer again, select the option, and click **Modify**.

By default, the SafeNet KSP utilities are installed in <client_install_dir>/KSP. The installation includes the following utilities:

- > **"kspcmd" below**
 - "Configuring the KSP Using the Command Line" on the next page
- > **"KspConfig" on page 401**
 - "Configuring the KSP Using the GUI" on page 401
- > **"ms2Luna" on page 402** — Used to migrate Microsoft CSP keys to a SafeNet Luna PCIe HSM partition
- > **"ksputil" on page 403** — Used to display and manage partition keys that are visible to the KSP

kspcmd

You can use this utility (<client_install_dir>/KSP/kspcmd.exe) to register the KSP library and partitions via the Windows command line.

NOTE To register the library and partitions using a GUI, use **"KspConfig" on page 401**. It is unnecessary to use both utilities.

Syntax

kspcmd.exe

library <path\cryptoki.dll>
password /s <slot_label> [/u <username>] [/d <domain>]
usagelimit
viewslots

Argument	Shortcut	Description
library <path\cryptoki.dll>	l	Register the library and associated provider names with KSP.
password	p	Register the designated slot and its Crypto Officer password/challenge to the KSP. You can specify the following options: /s <slot_label> [Mandatory] The label of the partition being registered to the KSP. /u <username> [Optional] The username to register for this partition. If this is not specified, all users on the client will be able to access this partition via KSP. /d <domain> [Optional] The domain to register for this partition.
usagelimit	u	Set the maximum usage limit for RSA keys using KSP. Enter 0 to register unlimited uses.
viewslots	v	Display the registered slots by user/domain.

Configuring the KSP Using the Command Line

You can use the **"kspcmd" on the previous page** command-line tool to configure the KSP for use with your partitions. The Crypto Officer must complete this procedure using Administrator privileges on the client.

You can register the following user/domain combinations with the KSP:

- > **Administrator** user with the domain specific to the client. Default Windows domains are in the format **WIN-XXXXXXXXXX**.
- > **SYSTEM** user with the **NT-AUTHORITY** domain

The configuration tool registers a Crypto Officer password/challenge to a specific user, so that only that user can unlock the partition.

To configure the KSP using the command line

1. In a command line, navigate to the SafeNet KSP install directory and register the **cryptoki.dll** library to the KSP.
"kspcmd" on the previous page **library /s** <path\cryptoki.dll> [/u <username>] [/d <domain>]
2. Register the designated slot and its Crypto Officer password/challenge to the KSP.
"kspcmd" on the previous page **password /s** <slot_label> [/u <username>] [/d <domain>]
You are prompted to enter the CO password/challenge for the slot.
3. [Optional] Display the registered slots to ensure that registration is complete.

"kspcmd" on page 399 viewslots

4. [Optional] Set the maximum usage limit for RSA keys using KSP.

"kspcmd" on page 399 usagelimit

You are prompted to enter a usage limit. Enter **0** to register unlimited uses.

KspConfig

You can use this tool (<client_install_dir>\KSP\KspConfig.exe) to register the KSP library and partitions using a GUI.

NOTE To register the library and partitions using the command line, use **"kspcmd" on page 399**. It is unnecessary to use both utilities.

Configuring the KSP Using the GUI

You can use the **"KspConfig" above** utility to configure the KSP for use with your partitions. The Crypto Officer must complete this procedure using Administrator privileges on the client.

You can register the following user/domain combinations with the KSP:

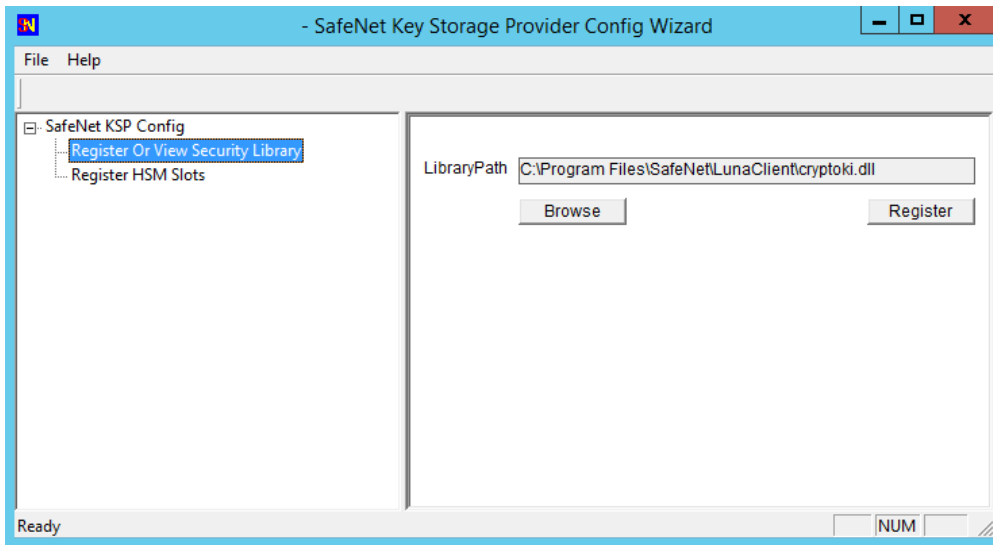
- > **Administrator** user with the domain specific to the client. Default Windows domains are in the format **WIN-XXXXXXXXXX**.
- > **SYSTEM** user with the **NT-AUTHORITY** domain

The configuration tool registers a Crypto Officer password/challenge to a specific user, so that only that user can unlock the partition.

To configure the KSP using the GUI

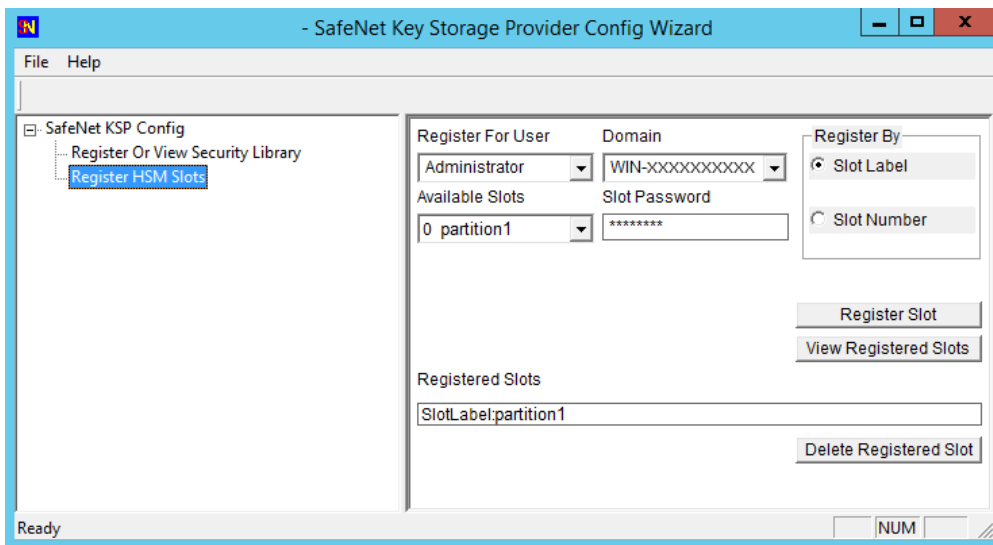
1. In Windows Explorer, navigate to the SafeNet KSP install directory and launch **"KspConfig" above** as the **Administrator** user.
2. In the left panel, double-click **Register or View Security Library**. Enter the filepath to **cryptoki.dll** or click Browse to locate it.

<client_install_dir>\cryptoki.dll



Click **Register** to complete the registration.

3. In the left panel, double-click **Register HSM Slots**. Select the **Administrator** user, client domain, and an available slot to register. Enter the CO password/challenge and click **Register Slot**.



4. Select the **SYSTEM** user and **NT-AUTHORITY** domain and register for the slot.
5. Repeat steps 3-4 for any other available slots you want to register with the KSP.

You can now begin using your applications to perform crypto operations on the registered slots.

ms2Luna

Use the **ms2Luna** utility (<client_install_dir>/KSP/ms2Luna.exe) to migrate existing Microsoft KSP keys held in software to a registered partition/HA group on the SafeNet Luna PCIe HSM. It requires the thumbprint of a certificate held in the client's keystore.

Prerequisites

- > You must already have registered a partition/HA group using the ["kspcmd" on page 399](#) or ["KspConfig" on page 401](#) utility.
- > Private keys must be exportable to be migrated to the HSM.

To migrate Microsoft KSP keys to the SafeNet Luna PCIe HSM

1. In a command prompt, navigate to the SafeNet KSP install directory and migrate your existing keys to the HSM.

ms2Luna

You are prompted for the KSP certificate thumbprint.

ksputil

KSP binds machine keys to the hostname of the crypto server that created the keys. You can use the ["ksputil" above](#) utility to display and manage keys that are visible to the KSP.

Syntax

ksputil

clusterkeys /s <slotnum> **/n** <keyname> **/t** <target>

listkeys /s <slotnum> **/user**

Argument	Shortcut	Description
clusterkeys	c	<p>Bind a specified keypair to a different server domain. Note that this does not change the bindings of existing keys; it creates a copy of the original keypair that is bound to the new domain.</p> <p>Available options:</p> <p>/s <slotnum> [Mandatory] The slot number of the partition where the key(s) are located.</p> <p>/n <keyname> [Mandatory] The name of the key(s) to bind to the new domain.</p> <p>/d <domain> [Mandatory] The domain to which keys will be bound.</p>
listkeys	l	<p>Display a list of KSP-visible keys.</p> <p>Available options:</p> <p>/s <slotnum> [Mandatory] The slot number of the partition where the key(s) are located.</p> <p>/user [Optional] List keys bound to the currently logged-in user/hostname.</p>

Algorithms Supported

Here, for comparison, are the algorithms supported by our CSP and KSP APIs.

Algorithms supported by the SafeNet CSP

CALG_RSA_SIGN
CALG_RSA_KEYX
CALG_RC2
CALG_RC4
CALG_RC5
CALG_DES
CALG_3DES_112
CALG_3DES
CALG_MD2
CALG_MD5
CALG_SHA
CALG_SHA_256
CALG_SHA_384
CALG_SHA_512
CALG_MAC
CALG_HMAC

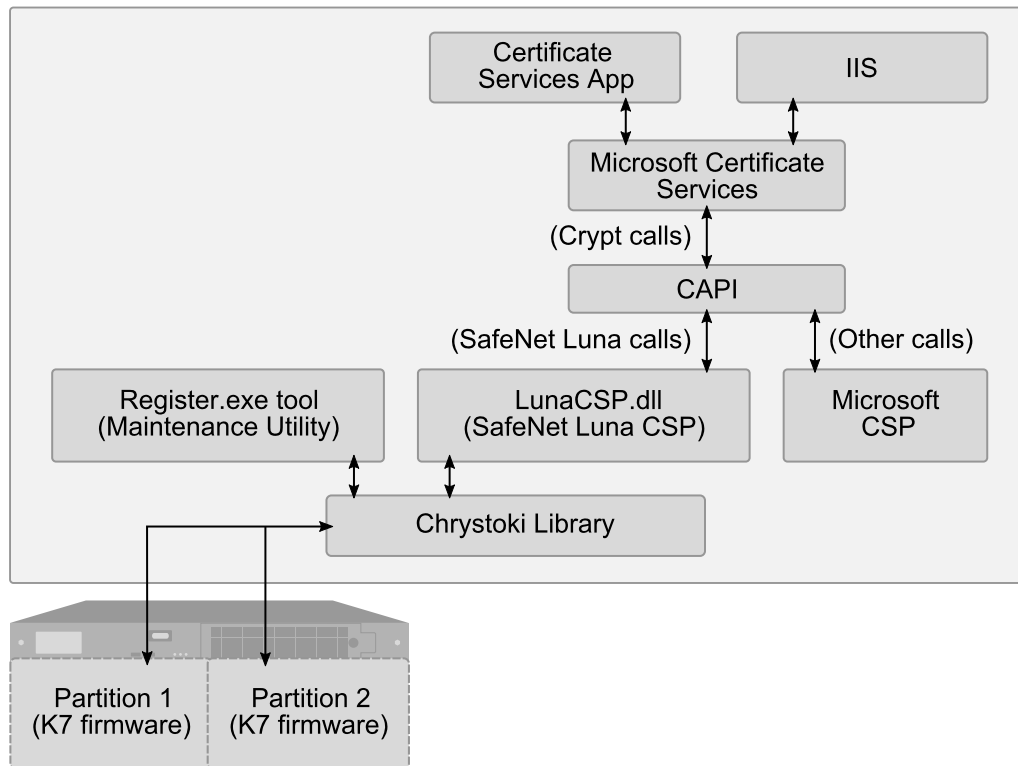
Algorithms supported by the SafeNet KSP

NCRYPT_RSA_ALGORITHM
NCRYPT_DSA_ALGORITHM
NCRYPT_ECDSA_P256_ALGORITHM
NCRYPT_ECDSA_P384_ALGORITHM
NCRYPT_ECDSA_P521_ALGORITHM
NCRYPT_ECDH_P256_ALGORITHM
NCRYPT_ECDH_P384_ALGORITHM
NCRYPT_ECDH_P521_ALGORITHM
NCRYPT_DH_ALGORITHM
NCRYPT_RSA_ALGORITHM

SafeNet CSP Calls and Functions

For integration with Microsoft Certificate Services and other applications, the LunaCSP.dll library accepts Crypt calls and gives access to token functions (via CP calls) as listed in this section. Key pairs and certificates are generated, stored and used on the SafeNet Luna PCIe HSM.

The diagram below depicts the relationship of the SafeNet components to the other layers in the certificate system.

Figure 1: SafeNet CSP architecture

Note, in the diagram, that the SafeNet CSP routes relevant calls through the statically linked Crystoki library to the HSM via CP calls. Other calls from the application layer – those not directed at the token/HSM, and not matching the SafeNet CSP supported functions (see next section) – are passed to the Microsoft CSP.

Programming for SafeNet Luna PCIe HSM with SafeNet CSP

The SafeNet CSP DLL exports the following functions, each one corresponding to an equivalent (and similarly named) Crypt call from the application layer:

- > CPAcquireContext
- > CPGetProvParam
- > CPSetProvParam
- > CPReleaseContext
- > CPDeriveKey
- > CPDestroyKey
- > CPDuplicateKey
- > CPExportKey
- > CPGenKey
- > CPGenRandom
- > CPGetKeyParam
- > CPGetUserKey

- > CPlmportKey
- > CPSetKeyParam
- > CPDecrypt
- > CPEncrypt
- > CPCreateHash
- > CPDestroyHash
- > CPGetHashParam
- > CPHashData
- > CPHashSessionKey
- > CPSetHashParam
- > CPSignHash
- > CPVerifySignature

NOTE The CPVerifySignature function is able to verify signatures of up to 2048 bits, regardless of the size of the signatures produced by CPSignHash. This ensures that the CSP is able to validate all compatible certificates, even those signed with large keys.

The MSDN (Microsoft Developers Network) web site provides syntax and descriptions of the corresponding Crypt calls that invoke the functions in the above list.

Algorithms

SafeNet CSP supports the following algorithms:

- > CALG_RSA_SIGN [RSA Signature] [256 - 4096 bits]. The CSP uses the RSA Public-Key Cipher for digital signatures.
- > CALG_RSA_KEYX [RSA Key Exchange] [256- 4096 bits] The CSP must use the RSA Public-Key Cipher key exchange. The exchange key pair can be used both to exchange session keys and to verify digital signatures.
- > CALG_RC2 [RSA Data Securities RC2 (block cipher)] [8 - 1024 bits].
- > CALG_RC4 [RSA Data Securities RC4 (stream cipher)] [8 - 2048 bits].
- > CALG_RC5 [RSA Data Securities RC5 (block cipher)] [8 - 2048 bits].
- > CALG_DES [Data Encryption Standard (block cipher)] [56 bits].
- > CALG_3DES_112 [Double DES (block cipher)] [112 bits].
- > CALG_3DES [Triple DES (block cipher)] [168 bits].
- > CALG_MAC [Message Authentication Code] (with RC2 only).
- > CALG_HMAC [Hash-based MAC].
- > CALG_MD2 [Message Digest 2 (MD2)] [128 bits].
- > CALG_MD5 [Message Digest 5 (MD5)] [128 bits].
- > CALG_SHA [Secure Hash Algorithm (SHA-1)] [160 bits].

- > CALG_SHA224 [Secure Hash Algorithm (SHA-2)] [224 bits].
- > CALG_SHA256 [Secure Hash Algorithm (SHA-2)] [256 bits].
- > CALG_SHA384 [Secure Hash Algorithm (SHA-2)] [384 bits].
- > CALG_SHA512 [Secure Hash Algorithm (SHA-2)] [512 bits].

NOTE If you intend to perform key exchanges between the SafeNet CSP and the Microsoft CSP with RC2 keys, the attribute `KP_EFFECTIVE_KEYLEN` must be set to 128 bits. For RC2 and RC4, the salt value of the keys must be transferred by making a call to get the salt value of the original key and to set the salt value of an imported key. This is done with the `CryptGetKeyParam(KP_SALT)` and `CryptSetKeyParam(KP_SALT)` functions respectively.