nShield Security World

nShield Cryptographic API v12.50.4 Integration Guide

4 March 2024

Contents

1 Introduction

This guide describes the following toolkits, supplied by nCipher to help developers write applications that use nShield modules:

- nCipher PKCS #11 library
- Cryptographic Hardware Interface Library
- Microsoft CryptoAPI (MSCAPI)
- Microsoft Cryptography API: Next Generation (CNG)
- nCipherKM JCA/JCE cryptographic service provider.

These tool kits, like the application plug-ins supplied by nCipher, use the Security World paradigm for key storage. For an introduction to Security Worlds, see the User Guide.

1.1 Read this guide if ...

Read this guide if you want to build an application that uses a nCipher key-management module to accelerate cryptographic operations and protect cryptographic keys through a standard interface rather than the full nCore API.

This guide assumes that you are familiar with the concept of the Security World, described in the User Guide. It is intended for experienced programmers and assumes that you are familiar with the following documentation:

- The *nCore Developer Tutorial*, which describes how to write applications using an nShield module
- The *nCore API Documentation* (supplied as HTML), which describes the nCore API.

1.2 Conventions

1.2.1 Typographical conventions

ℹ This symbol indicates important supplemental information.

🔒 This symbol is used to indicate if there is a danger of loss or exposure of key material (or any other security risk).

Keyboard keys that you must press are represented like this: `Enter`, `Ctrl-C`.

Examples of onscreen text from graphical user interfaces are represented by **boldface** text. Names of files, command-line utilities, and other system items are represented in **`monospace`** text. Variable text that you either see onscreen or that you must enter is represented in *italic*.

Examples of onscreen terminal display, both of data returned and of your input, are represented in a form similar to the following:

```
install
```

1.2.2 CLI command conventions

The basic syntax for a `CLI` command is:

```
command object <object_name> [parameter] [option] [modifier]
```

In this syntax, user-defined values are shown in *italics* and enclosed within the **< >** characters. Optional elements are shown enclosed within the **[ ]** characters. Mutually exclusive elements are separated by the **|** character.

Many system objects require the inclusion of a user-defined keyword value. For example, the **user** object is executed against a user-supplied *user_name*. Throughout this guide, all user-defined keyword values are shown in *italics*.

Each `CLI` command that you run performs an operation against the internal configuration of the appliance. The specific type of operation is specified by the first user-defined keyword value in the command string.

1.2.3 Model numbers

Model numbering conventions are used to distinguish different nCipher hardware security devices. In the table below, *n* represents any single-digit integer.

Model number	Used for
NH2047	nShield Connect 6000
NH2040	nShield Connect 1500
NH2033	nShield Connect 500
NH2068	nShield Connect 6000+
NH2061	nShield Connect 1500+
NH2054	nShield Connect 500+
NH2075-B	nShield Connect XC Base
NH2075-M	nShield Connect XC Medium
NH2075-H	nShield Connect XC High
NH2082	nShield Connect XC SCAP
nC2021E-000, NCE2023E-000	nToken PCIe
nC3*nnn*E-*nnn*, nC4*nnn*E-*nnn*	nCipher nShield Solo PCIe
nC30n5E-*nnn*, nC40n5E-*nnn*	nCipher nShield Solo XC PCIe
nC30*nn*U-10, nC40*nn*U-10.	nShield Edge

1.2.4 Security World Software

1.2.4.1 Default directories

The default locations for Security World Software and program data directories on English-language systems are summarized in the following table:

Directory name	Environment variable	Windows Server 2008 or later	Unix-based
nShield Installation	`NFAST_HOME`	32 bit: `C:\Program Files\nCipher\nfast` 64 bit: `C:\Program Files (x86)\nCipher\nfast`	`/opt/nfast/`
Key Management Data	`NFAST_KMDATA`	`C:\ProgramData\nCipher\Key Management Data`	`/opt/nfast/kmdata/`
Dynamic Feature Certificates	`NFAST_CERTDIR`	`C:\ProgramData\nCipher\Feature Certificates`	`/opt/nfast/femcerts/`
Static Feature Certificates		`C:\ProgramData\nCipher\Features`	`/opt/nfast/kmdata/features/`
Log Files	`NFAST_LOGDIR`	`C:\ProgramData\nCipher\Log Files`	`/opt/nfast/log/`

ℹ By default, the Windows *%NFAST_KMDATA%* directories are hidden directories. To see these directories and their contents, you must enable the display of hidden files and directories in the View settings of the Folder Options.

ℹ Dynamic feature certificates must be stored in the directory stated above. The directory shown for static feature certificates is an example location. You can store those certificates in any directory and provide the appropriate path when using the Feature Enable Tool. However, you must not store static feature certificates in the dynamic features certificates directory. For more information about feature certificates, see the *User Guide* for your HSM.

The absolute paths to the Security World Software installation directory and program data directories on Windows platforms are stored in the indicated nShield environment variables at the time of installation. If you are unsure of the location of any of these directories, check the path set in the environment variable.

The instructions in this guide refer to the locations of the software installation and program data directories by their names (for example, Key Management Data) or:

- For Windows, nShield environment variable names enclosed with percent signs (for example, *%NFAST_KMDATA%*)
- For Unix-based systems, absolute paths (for example, `/opt/nfast/kmdata/`).

If the software has been installed into a non-default location:

- For Windows, ensure that the associated nShield environment variables are re-set with the correct paths for your installation
- For Unix-based systems, you must create a symbolic link from `/opt/nfast/` to the directory where the software is actually installed; for more information about creating symbolic links, see your operating system's documentation.

> With previous versions of Security World Software for Windows platforms, the Key Management Data directory was located by default in `C:\nfast\kmdata`, the Feature Certificates directory was located by default in `C:\nfast\fem`, and the Log Files directory was located by default in `C:\nfast\log`.

1.2.4.2 Utility help options

Unless noted, all the executable utilities provided in the `bin` subdirectory of your nShield installation have the following standard help options:

`-h|--help` displays help for the utility

`-v|--version` displays the version number of the utility

`-u|--usage` displays a brief usage summary for the utility.

1.2.5 Document version numbers

The version number of this document is shown on the copyright page of this guide. Quote the version number and the date on the copyright page if you need to contact Support about this document.

1.3 Further information

This guide forms one part of the information and support provided by nCipher. You can find additional documentation in the `document` directory of the installation media for your product.

The *nCore API Documentation* is supplied as HTML files installed in the following locations:

- Windows:
  - API reference for host: *%NFAST_HOME%*`\document\ncore\html\index.html`
  - API reference for SEE: *%NFAST_HOME%*`\document\csddoc\html\index.html`
- Unix-based:
  - API reference for host:`/opt/nfast/document/ncore/html/index.html`
  - API reference for SEE:`/opt/nfast/document/csddoc/html/index.html`

The Java Generic Stub classes, nCipherKM JCA/JCE provider classes, and Java Key Management classes are supplied with HTML documentation in standard **`Javadoc`** format, which is installed in the appropriate `nfast\java` or `nfast/java` directory when you install these classes.

Release notes containing the latest information about your product are available in the `release` directory of your installation media.

ℹ We strongly recommend familiarizing yourself with the information provided in the release notes before using any hardware and software related to your product.

1.4 Security advisories

If nCipher becomes aware of a security issue affecting nShield HSMs, nCipher will publish a security advisory to customers. The security advisory will describe the issue and provide recommended actions. In some circumstances the advisory may recommend you upgrade the nShield firmware and or nShield Connect image file. In this situation you will need to re-present a quorum of administrator smart cards to the HSM to reload a Security World. As such, deployment and maintenance of your HSMs should consider the procedures and actions required to upgrade devices in the field.

ℹ The Remote Administration feature supports remote firmware upgrade of nShield Solo and nShield Connects and remote ACS card presentation.

We recommend that you monitor the "nShield Announcements & Security Notices" section of the nCipher Security Support Portal, where any announcement of nShield Security Advisories will be made.

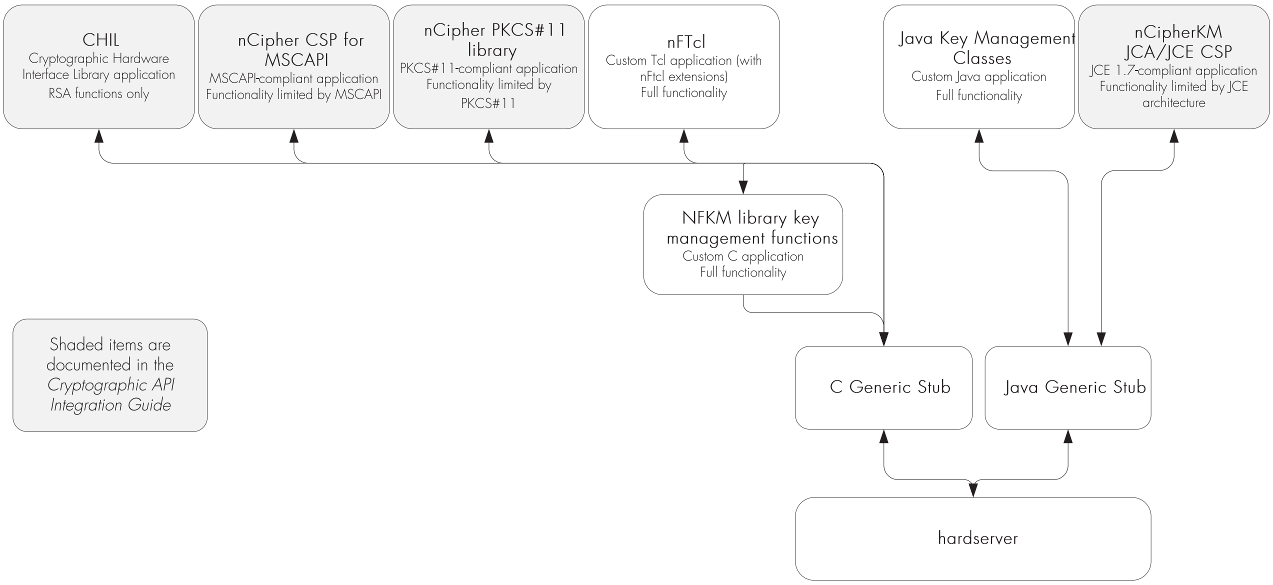
1.4.1 Contacting nCipher Support

To obtain support for your product, visit: https://help.ncipher.com.

2 nShield architecture

This chapter provides a brief overview of the Security World Software architecture. For a visual representation of nShield architecture and the documentation that relates to it, see Figure 1.

Figure 1. nShield Architecture


CHIL
Cryptographic Hardware Interface Library application
RSA functions only
nCipher CSP for MSCAPI
MSCAPI-compliant application
Functionality limited by MSCAPI
nCipher PKCS#11 library
PKCS#11-compliant application
Functionality limited by PKCS#11
nFTcl
Custom Tcl application (with nFtcl extensions)
Full functionality
Java Key Management Classes
Custom Java application
Full functionality
nCipherKM JCA/JCE CSP
JCE 1.7-compliant application
Functionality limited by JCE architecture
NFKM library key management functions
Custom C application
Full functionality
Shaded items are documented in the *Cryptographic API Integration Guide*
C Generic Stub
Java Generic Stub
hardserver

2.1 Security World Software modules

nShield modules provide a secure environment to perform cryptographic functions. Key-management modules are fitted with a smart card interface that enables keys to be stored on removable tokens for extra security. nShield modules are available for PCI buses and also as network attached Ethernet modules (nShield Connect).

2.2 Security World Software server

The Security World Software server, often referred to as the **hardserver**, accepts requests by means of an interprocess communication facility (for example, a Unix domain socket on Unix or named pipes or TCP/IP sockets on Windows).

The Security World Software server receives requests from applications and passes these to the nShield module(s). The module handles these requests and returns them to the server. The server ensures that the results are returned to the correct calling program.

You only need a single Security World Software server running on your host computer. This server can communicate with multiple applications and multiple nShield modules.

2.3 Stubs and interface libraries

An application can either handle its own cryptographic functions or it can use a cryptographic library:

- If the application uses a cryptographic library that is already able to communicate with the Security World Software server, then no further modification is necessary. The application can automatically make use of the nShield module.
- If the application uses a cryptographic library that has not been modified to be able to communicate with the Security World Software server, then either nCipher or the cryptographic library supplier need to create adaption function(s) and compile them into the cryptographic library. The application users then must relink their applications using the updated cryptographic library.

If the application performs its own cryptographic functions, you must create adaption function(s) that pass the cryptographic functions to the Security World Software server. You must identify each cryptographic function within the application and change it to call the nShield adaption function, which in turn calls the generic stub. If the cryptographic functions are provided by means of a DLL or shared library, the library file can be changed. Otherwise, the application itself must be recompiled.

2.4 Using an interface library

nCipher supplies the following interface libraries:

- Cryptographic Hardware Interface Library
- Microsoft CryptoAPI
- PKCS #11
- nCipherKM JCA/JCE CSP

Third-party vendors may supply nShield-aware versions of their cryptographic libraries.

The functionality provided by these libraries is the intersection of the functionality provided by the nCore API and the functionality provided by the standard for that library.

Most standard libraries offer fewer key-management options than are available in the nCore API. However, the nShield libraries do not include any extensions to their standards. If you want to make use of features of the nCore API that are not offered in the standard, you should convert your application to work directly with the generic stub.

On the other hand, many standard libraries include functions that are not supported on the nShield module, such as support for IDEA or Skipjack. If you require a feature that is not supported on the nShield module, contact Support because it may be possible to add the feature in a future release. However, in many cases, features are not present on the module for licensing reasons, as opposed to technical reasons, and nCipher cannot offer them in the interface library.

2.5 Writing a custom application

If you choose not to use one of the interface libraries, you must write a custom application. This gives you access to all the features of the nCore API. For this purpose, nCipher provides generic stub libraries for C and Java, as well as a set of Tcl extensions that call the C generic stub library. If you want to use a language other than C, Java, or Tcl, you must write your own wrapper functions in your chosen programming language that call the C generic stub functions.

nCipher supplies several utility functions to help you write your application.

2.6 Acceleration-only or key management

You must also decide whether you want to use key management or whether you are writing an acceleration-only application.

Acceleration-only applications are much simpler to write but do not offer any security benefits.

The nShield Cryptographic Hardware Interface Library, Microsoft CryptoAPI, Java JCE, PKCS #11, as well as the application plug-ins, use the Security World paradigm for key storage.

If you are writing a custom application, you have the option of using the Security World mechanisms, in which case your users can use either KeySafe or the command-line utilities supplied with the module for many key-management operations. This means you do not have to write these functions yourself.

The NFKM library gives you access to all the Security World functionality.

3 PKCS #11

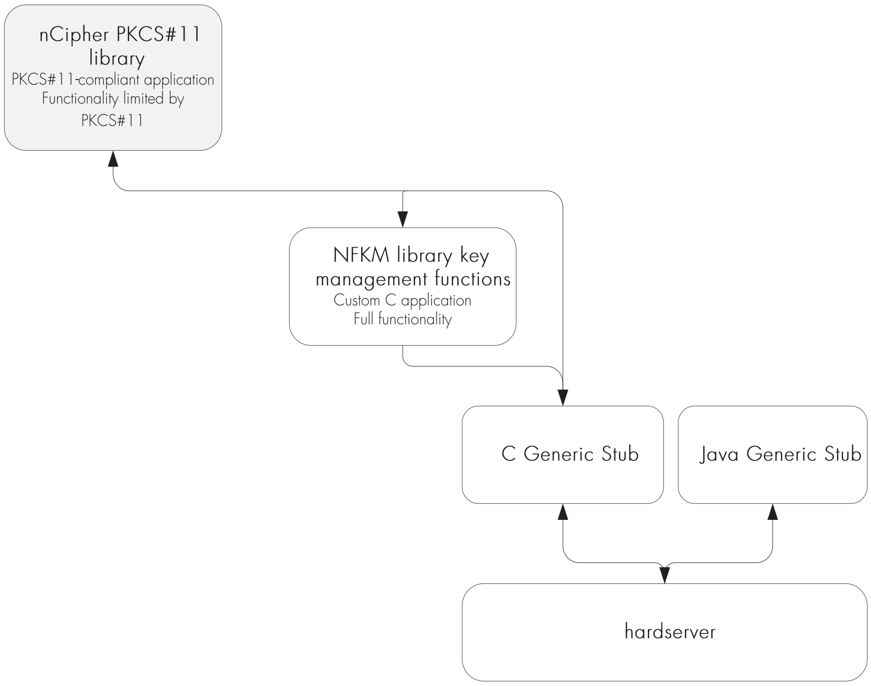
This chapter is intended for application developers who are writing PKCS #11 applications.

For an introduction to the PKCS #11 user library, including information about the environment variables and utilities available, see the *User Guide* for your HSM.

Before using the nCipher PKCS #11 libraries, we recommend that you read the *PKCS #11: Cryptographic Token Interface Standard*, version 2.01, published by RSA Laboratories.

For an illustration of the way that an nCipher PKCS #11 library works with the nShield APIs, see Figure 2.

Figure 2. nCipher PKCS #11 architecture



This guide does not address how the nCipher PKCS #11 libraries map PKCS #11 functions to nCore API calls within the library.

3.1 PKCS #11 developer libraries

The nCipher PKCS #11 libraries, `cknfast.lib` (`libcknfast.a` on Unix-based systems) are provided so that you can integrate your PKCS #11 applications with the nShield hardware security modules.

The nCipher PKCS #11 libraries:

- Provide the PKCS #11 mechanisms listed in *Mechanisms* on page 35
- Help you to identify potential security weaknesses, enabling you to create secure PKCS #11 applications more easily.

3.1.1 PKCS #11 security assurance mechanism

It is possible for an application to use the PKCS #11 API in ways that can introduce potential security weaknesses. For example, it is a requirement of the PKCS #11 standard that the nCipher PKCS #11 libraries are able to generate keys that are explicitly exportable in plain text. An application could use this ability in error when a secure key would be more appropriate.

The nCipher PKCS #11 libraries are provided with a configurable security assurance mechanism (SAM). SAM helps prevent PKCS #11 applications from performing operations through the PKCS #11 API that may compromise the security of cryptographic keys. Operations that reveal questionable behavior by the application fail by default with an explanation of the cause of failure.

If you decide that some operations that carry a higher security risk are acceptable to you, then you can reconfigure the nCipher PKCS #11 library to permit these operations by means of the environment variable **`CKNFAST_OVERRIDE_SECURITY_ASSURANCES`**. You must think carefully, however, before permitting operations that could compromise the security of cryptographic keys. For more information about the environment variable and its parameters, see the *User Guide* for your HSM.

It is your responsibility as a security developer to familiarize yourself with the PKCS #11 standard and to ensure that all cryptographic operations used by your application are implemented in a secure manner.

If no parameters are supplied to the environment variable, the nCipher PKCS #11 library fails and issues a warning, with an explanation, when the following operations are detected:

- Short term session keys created as long term objects
- Keys that can be exported as plain text are created
- Keys are imported from external sources
- Wrapping keys are created or imported
- Unwrapping keys are created or imported
- Keys with weak algorithms (for example, DES) are created
- Keys with short key length are created.

3.2 PKCS #11 with load-sharing mode

The behavior of the nCipher PKCS #11 library varies depending on which of load-sharing mode, HSM Pool mode or neither or these is enabled. If you have enabled load sharing mode, the nCipher PKCS #11 library creates one virtual slot for each OCS and, optionally, also creates one slot for the module (or modules). Softcards appear as additional virtual slots once enabled.

Load-sharing mode must be enabled in PKCS #11 in order to use softcards.

Whether or not load-sharing mode is enabled is determined by the state of the **`CKNFAST_LOADSHARING`** environment variable.

Load-sharing mode enables you to load a single PKCS #11 token onto several nShield modules to improve performance. To enable successful load-sharing with an OCS protected key:

- You must have an Operator Card from the OCS inserted into every slot from the same 1/*N* card set
- All the Operator Cards must have the same pass phrase.

The nShield-specific API calls, **`C_LoginBegin`**, **`C_LoginNext`**, and **`C_LoginEnd`** do not function in load-sharing mode. *K*/*N* support for card sets in load-sharing mode is only available if you first use **`preload`** to load the logical token.

3.2.1 Logging in

If you call **`C_Login`** without a token present, it fails (as expected) unless you are using a persistent token with **`preload`** or using only module protected keys. Therefore, your application should prompt users to insert tokens before logging in.

The nCipher PKCS #11 library removes the nShield logical token when you call **`C_Logout`**, whether or not there is a smart card in the reader.

If there are any cards from the OCS present when you call **`C_Logout`**, the PKCS #11 token remains present but not logged-in until all cards in the set are removed. If there are no cards present, the PKCS #11 token becomes not present.

The **`CKNFAST_NONREMOVABLE`** environment variable is only available for persistent tokens. When the variable is set, the rules for recognizing new cards are overridden, and the only way to invoke a new token is to call **`C_Finalize`** or **`C_Initialize`**.

3.2.2 Session objects

Session objects are loaded on all modules.

3.2.3 Module failure

If a subset of the modules fails, the nCipher PKCS #11 library handles commands using the remaining modules. If a module fails, the single cryptographic function that was running on that module will fail, and the nCipher PKCS #11 library will return a PKCS #11 error. Subsequent cryptographic commands will be run on other modules.

3.2.4 Compatibility

Before the implementation of load-sharing, the nCipher PKCS #11 library put the electronic serial number in both the **`slotinfo.slotDescription`** and **`tokeninfo.serialNumber`** fields. If you have enabled load-sharing, the **`tokeninfo.serialNumber`** field displays the hash of the OCS.

3.2.5 Restrictions on function calls in load-sharing mode

The following function calls are not supported in load-sharing mode:

- **`C_LoginBegin`** (nShield-specific call to support *K*/*N* card sets)
- **`C_LoginNext`** (nShield-specific call to support *K*/*N* card sets)
- **`C_LoginEnd`** (nShield-specific call to support *K*/*N* card sets).

The following function calls are supported in load-sharing mode *only* when using softcards:

- `C_InitToken`
- `C_InitPin`
- `C_SetPin`.

To use `C_InitToken`, `C_InitPin`, or `C_SetPin` in load-sharing mode, you must have created a softcard with the command `ppmk -n` before selecting the corresponding slot.

The `C_InitToken` function is *not* supported for use in non-load-sharing FIPS 140-2 level 3 Security Worlds.

3.3 PKCS #11 with HSM Pool mode

If HSM Pool mode is enabled, the nCipher PKCS #11 library exposes a single pool of HSMs and a single virtual slot for a fixed token with the label `accelerator`. This accelerator slot can be used to create module protected keys and to support session objects.

HSM Pool mode supports module protected keys but does not support token protected keys. If your application only uses module protected keys, you can use HSM Pool mode as an alternative to using load-sharing mode. HSM Pool mode supports returning or adding a hardware security module to the pool without restarting the system.

Whether or not HSM Pool mode is enabled is determined by the state of the `CKNFAST_HSM_POOL` environment variable.

In FIPS 140-2 level 3 Security Worlds, keys cannot be created in HSM Pool mode, however keys created outside HSM Pool mode can be used in HSM Pool mode.

3.3.1 Module failure

If a subset of the modules in the HSM pool fail, the nCipher PKCS #11 library handles commands using the remaining modules. When a module fails, any cryptographic functions that were running on that module are restarted on one of the remaining modules. If all of the modules in the HSM pool fail, the nCipher PKCS #11 library will return a PKCS #11 error.

3.3.2 Module recovery

If a failed module recovers and remains part of the Security World, it is automatically returned to the HSM Pool and the nCipher PKCS #11 library can use it for new commands. If a new module is added to the system that is accessible to the host running the PKCS #11 application, then once the Security World has been loaded onto this module, then it is automatically added to the HSM Pool and the nCipher PKCS #11 library can use it for new commands.

3.3.3 Restrictions on function calls in HSM Pool mode

The following function calls are not supported in HSM Pool mode:

- `C_LoginBegin`
- `C_LoginNext`

- **C_LoginEnd**
- **C_InitToken**
- **C_InitPin**
- **C_SetPin**

3.4 PKCS #11 without load-sharing mode or HSM Pool mode

The nCipher PKCS #11 library makes each nShield module appear to your PKCS #11 application as two or more PKCS #11 slots.

The first slot represents the module itself. This token:

- Appears as a non-removable hardware token and has the flag **CKF_REMOVABLE** not set
- Has the flag **CKF_LOGIN_REQUIRED** not set (**C_Login** always fails on this flag).

Applications can ignore this slot, but you can use the slot to store public session objects or for functions that do not use objects (such as **C_GenerateRandom**) even when the smart-card is not present.

The second slot represents the smart-card reader. This token:

- appears as a PKCS #11 slot, potentially containing a removable hardware token that has the flag **CKF_REMOVABLE** set
- is marked as removed if the smart card is removed from the physical slot
- has the flag **CKF_LOGIN_REQUIRED**
- allows the creation of token objects.

To use softcards with PKCS #11, load-sharing mode must be enabled.

A PKCS #11 token can support multiple concurrent sessions on multiple applications. However, by default, only one token may be logged in to a given slot at a given time (see *K/N support for PKCS #11* on page 23). By default, when you insert a new card into a slot, the nCipher PKCS #11 library automatically logs out any token that had been logged in to the slot previously.

The **C_InitToken** function is *not* supported for use in non-load-sharing FIPS 140-2 level 3 Security Worlds.

3.4.1 K/N support for PKCS #11

If you use the nCipher PKCS #11 library without load-sharing mode or HSM Pool mode, you can implement *K/N* card set support in two ways:

- By using the nShield-specific API calls, **C_LoginBegin**, **C_LoginNext**, and **C_LoginEnd**
- By using the **preload** command-line utility to load the logical token first.

3.5 Generating and deleting NVRAM-stored keys with PKCS #11

You can use the nCipher PKCS #11 library to generate keys stored in nonvolatile memory (up to a maximum of 12 keys) if you have set the **CKNFAST_NVRAM_KEY_STORAGE** environment variable.

3.5.1 Generating NVRAM-stored keys

To generate NVRAM-stored keys with the nCipher PKCS #11 library:

1. Load (or reload) the ACS using the **preload** command-line utility. Open a command-line window and give the command:

   ```
   preload --admin=NV pause
   ```

2. After loading the ACS, remove the Administrator Cards from the module.
3. Ensure that the **CKNFAST_NVRAM_KEY_STORAGE** environment variable is set. If this variable is not set, the keys generated are not stored in NVRAM.
4. Open a second command-line window, and give the command:

   ```
   preload --cardset-name=name pkcs11app
   ```

   where *name* is the cardset name and *pkcs11app* is the name of your PKCS #11 application.

5. Generate the NVRAM-stored keys that you need (up to a maximum of 12 keys) as normal.
6. Stop or close *pkcs11app*.
7. Return to the command-line window you opened in step 1 and terminate the **preload --admin=NV pause** process.

   Do not allow the **preload --admin=NV pause** process to run continuously. Run this process only when generating or deleting NVRAM-stored keys. As usual, remove the Administrator Cards when they are not in use and store them safely.

8. Unset the **CKNFAST_NVRAM_KEY_STORAGE** environment variable.
9. Restart *pkcs11app*.

   You can use the newly generated NVRAM-stored keys in the same way as other PKCS #11 keys. You can also generate any number of standard keys (not stored in NVRAM) in the usual way.

3.5.2 Deleting NVRAM-stored keys

To delete NVRAM-stored keys with the nCipher PKCS #11 library:

1. Load (or reload) the ACS using the **preload** command-line utility. Open a command-line window and give the command:

```
preload --admin=NV pause
```

2. After loading the ACS, remove the Administrator Cards from the module. Ensure that the **CKNFAST_NVRAM_KEY_STORAGE** environment variable is set.

   ℹ If you attempt to delete NVRAM-stored keys without the **CKNFAST_NVRAM_KEY_STORAGE** environment variable set, only the key blob stored on hard disk is deleted. The keys remain in NVRAM on the module. Use the **nvram-sw** command-line utility to fully remove the NVRAM-stored keys. For more information, see the *User Guide*.

3. Open a second command-line window, and give the command:

```
preload --cardset-name=name -M pkcs11app
```

   where *name* is the cardset name and *pkcs11app* is the name of the PKCS #11 application that you use to delete the keys.

4. Delete the NVRAM-stored keys as you would delete normal keys.
5. Stop or close *pkcs11app*.
6. Return to the command-line window you opened in step 1 and terminate the **preload --admin=NV pause** process.

   ℹ Do not allow the **preload --admin=NV pause** to run continuously. Run this process only when generating or deleting NVRAM-stored keys. As usual, remove the Administrator Cards when they are not in use and store them safely.

7. Unset the **CKNFAST_NVRAM_KEY_STORAGE** environment variable.

3.6 nShield-specific PKCS #11 API extensions

nShield *K/N* card sets use nShield-specific API calls. These calls can be used by the application in place of the standard **C_Login** to provide log-in to a card set with a K parameter greater than 1. The API calls include three functions, **C_LoginBegin**, **C_LoginNext** and **C_LoginEnd**.

ℹ The login sequence must occur in the same session.

ℹ You cannot use the API calls in load-sharing mode. To use *K/N* card sets in load-sharing mode, use **preload** to load the logical token first. The API calls also work in a non-load-sharing FIPS 140-2 level 3 Security Worlds.

3.6.1 C_LoginBegin

Similar to **C_Login**, this function initiates the log-in process, ensures that the session is valid, and ensures that the user is not in load-sharing mode.

The **pulK** and **pulN** return values provide the caller with the number of card requests required. An example of the use of **C_LoginBegin** is shown here:

```
C_LoginBegin (CK_SESSION_HANDLE hSession, /* the session's handle */
              CK_USER_TYPE userType, /* the user type */
              CK_ULONG_PTR pulK, /* cards required to load logical token*/
              CK_ULONG_PTR pulN /* Number of cards in set */)
```

3.6.2 C_LoginNext

C_LoginNext is called *K* times until the required number of cards (for the given card set) have been presented. This function checks the Security World info to ensure that the card has changed each time. It also checks for the correct pass phrase before loading the card share. **pulSharesLeft** allows the user application to assess the number of cards loaded to the number of cards required.

CK_RV gives various values that allow the user to access the application state using standard PKCS #11 return values (such as **CKR_TOKEN_NOT_RECOGNIZED**). These values reveal such information as whether the card is the same, whether the card is foreign or blank, and whether the pass phrase was incorrect.

An example of the use of **C_LoginNext** is shown here:

```
C_LoginNext (CK_SESSION_HANDLE hSession, /* the session's handle */
             CK_USER_TYPE userType, /* the user type*/
             CK_CHAR_PTR pPin, /* the user's PIN*/
             CK_ULONG ulPinLen, /* the length of the PIN */
             CK_ULONG_PTR pulSharesLeft /* Number of shares still needed */)
```

3.6.3 C_LoginEnd

C_LoginEnd is called after all the shares are loaded. It constructs the logical token from the presented shares and then loads the private objects protected by the card set that are available to it:

```
C_LoginEnd (CK_SESSION_HANDLE hSession, /* the session's handle */
            CK_USER_TYPE userType /* the user type*/)
```

There must be no other calls between the functions, in that or any other session on the slot. In particular, a call that updates the Security World while using a card that has been removed at the time (for example, because a second card from the set is about to be inserted) returns **CKR_DEVICE_REMOVED** in the same way that it would for a single card. All sessions are then closed and the log-in process is aborted.

If other functions are accidentally called during the log-in cycle, then **slot.loadcardsetstate** is checked before updating the Security World. If the log-in process has not been completed, other functions return **CKR_FUNCTION_FAILED** and allow you to continue with the log-in process.

3.7 Compiling and linking

The following options are available if you want to integrate the nCipher PKCS #11 library with your application. Depending on how your application integrates with PKCS #11 libraries, you can:

- statically link the nCipher PKCS #11 library directly into your application
- dynamically link the nCipher PKCS #11 library into your application
- create a plug-in shared library that contains the nShield position-independent code object files together with your own adaptation facilities.

You may freely supply your users with the compiled library files linked into your application or into a plug-in library used for your application.

The nCipher PKCS #11 library includes the PKCS #11 header files **`pkcs11.h`**, **`pkcs11t.h`**, and **`pkcs11f.h`** from the RSA Data Security, Inc. Cryptoki Cryptographic Token Interface. Any work based on this interface is bound by the following terms of RSA Data Security, Inc. Licence, which states:

License is also granted to make and use derivative works provided that such works are identified as derived from the RSA Data Security, Inc. Cryptoki Cryptographic Token Interface in all material mentioning or referencing the derived work.

For more information about using the available libraries, see the **`Include Paths and Linking`** section in the *nCore API Documentation* on the Security World Software installation media.

3.7.1 Windows

All versions are built with Visual C++ 12.0. nCipher supplies the following files:

- *%NFAST_HOME%*`\bin\cknfast.dll` and *%NFAST_HOME%*`\toolkits\pkcs11\cknfast.dll`: a dynamically linked library

  Both files are identical.

- *%NFAST_HOME%*`\c\ctd\lib\cknfast.lib`: a stub for applications that link to **`cknfast.dll`**
- *%NFAST_HOME%*`\c\ctd\lib\libcknfast.lib`: a static library
- *%NFAST_HOME%*`\c\ctd\lib\libdcknfast.lib`: a static library with position-independent code
- *%NFAST_HOME%*`\c\ctd\lib\libtcknfast.lib`: a threadsafe library.

3.7.2 Unix-based

For each of the various supported Unix-based systems, nCipher supplies some or all of the following libraries:

- **`libcknfast.so`**, **`libcknfast.so.a`**, or **`libcnfast.sl`**: a standard, dynamically linked, shared library that can be used to create applications that must be dynamically linked with the nCipher libraries at run time. On platforms where thread safety requires programs to be compiled differently from non-threaded programs, these libraries are compiled thread-safe. On HP-UX and AIX, both threadsafe and non-threadsafe versions are provided. HP-UX also provides a packed library pragma; for more information about this see the RSA Laboratories PKCS #11 documentation.

- HP-UX
  - **`ansic-thr/lib/libcknfast.sl`** (threadsafe)
  - **`ansic/lib/libcknfast.sl`** (non-threadsafe)
  - **`ansic64-thr/lib/libcknfast.sl`** (threadsafe)
  - **`ansic64/lib/libcknfast.sl`** (non-threadsafe)
- AIX
  - **`xlc_r/lib/libcknfast.so.a`** (threadsafe)
  - **`xlc/lib/libcknfast.so.a`** (non-threadsafe)

  ℹ When using the 64-bit xlc_r64 utilities on AIX platforms, the NFAST_HOME/toolkits/PKCS#11/ directory contains both **`libcknfast.so.a`** (32-bit library) and **`libcknfast-64.so.a`** (64-bit library). The 32-bit library is incorrectly used instead of the 64-bit library. The workaround is to move the 32-bit library out of this directory, and then rename the 64-bit library to **`libcknfast.so.a`**.

- **`libcknfast.a`**: a standard, non-shared library used to statically link an application.
- **`libcknfast_thrpic.a`**: a non-shared library, compiled as threadsafe position-independent code.

On the Developer installation media, each library is provided with a corresponding set of header files. All the header files for each version are very similar, but some header files (particularly those that contain information about compiler and configuration options) differ by version.

These types of library are provided compiled with the following C compilers:

3.7.2.1 Solaris

Library type	Build notes
`/opt/nfast/c/ctd/gcc/lib`	This type of library is built with gcc 3.4.3.
`/opt/nfast/c/ctd/swspro/lib`	This type of library is built with Sun Workshop Compiler 5.0 (for Solaris 11).
`/opt/nfast/c/ctd/swspro64/lib`	This type of library is built with Sun Workshop Compiler 5.0 (for Solaris 11).

3.7.2.2 HP-UX

For HP-UX 11i v3, all of the following libraries are built with HP C/aC++ B3910B A.06.15 [May 16 2007]:

library type	Build notes
`/opt/nfast/c/ctd/ansic/lib`	This type of library is built for the ILP32 data model.
`/opt/nfast/c/ctd/ansic-thr/lib`	This type of library is built for the ILP32 data model and for threadsafe programs.
`/opt/nfast/c/ctd/ansic64/lib`	This type of library is built for the LP64 data model.
`/opt/nfast/c/ctd/ansic64-thr/lib`	This type of library is built for the LP64 data model and for threadsafe programs.

3.7.2.3 AIX

The following types of library are compiled on AIX 6.1 and are designed to be compatible with AIX 6.1 and AIX 7.1.

ℹ The libraries have not been optimised for the Power 8 architecture.

library type	Build notes
`/opt/nfast/c/ctd/xlc/lib`	This type of library is built with xlc (`/usr/vac/bin/xlc`) in 32-bit mode.
`/opt/nfast/c/ctd/xlc_r/lib`	This type of library is built with xlc_r (`/usr/vac/bin/xlc_r`) in 32-bit mode for threadsafe programs.
`/opt/nfast/c/ctd/xlc64/lib`	This type of library is built with xlc (`/usr/vac/bin/xlc`) in 64-bit mode.
`/opt/nfast/c/ctd/xlc_r64/lib`	This type of library is built with xlc_r (`/usr/vac/bin/xlc`) in 64-bit mode for threadsafe programs.

3.7.2.4 Linux libc6.11

library type	Build notes
`/opt/nfast/c/ctd/gcc/lib`	This type of library is built with gcc 4.9.2 in 32-bit mode.
`/opt/nfast/c/csd/gcc/lib`	This type of library is built with gcc 4.9.2 in 64-bit mode.

3.8 Objects

Token objects are not stored in the nShield module. Instead, they are stored in an encrypted and integrity-protected form on the hard disk of the host computer. The key used for this encryption is created by combining information stored on the smart card with information stored in the nShield module and with the card pass phrase.

Session keys are stored on the nShield module, while other session objects are stored in host memory. Token objects on the host are created in the **`kmdata`** directory.

In order to access token objects, the user must have:

- the smart card
- the pass phrase for the smart card
- an nShield module containing the module key used to create the token
- the host file containing the nShield key blob protecting the token object.

The nCipher PKCS #11 library can be used to manipulate Data Objects, Certificate Objects, and Key Objects.

3.8.1 Certificate Objects and Data Objects

The nCipher PKCS #11 library does not parse Certificate Objects or Data Objects.

The size of Data Objects is limited by what can be fitted into a single command (under most circumstances, this limit is 8192 bytes).

3.8.2 Key Objects

The following restrictions apply to keys.

Key types	Restrictions
RSA	Modulus greater than or equal to 1024. The nCipher PKCS #11 library requires all of the attributes for an RSA key object to be supplied, as listed in Table 27 of PKCS #11 Cryptographic Token Interface Standard version 2.01.
DSA	Modulus greater than or equal to 1024 in multiples of 8 bits.
Diffie-Hellman	Modulus greater than or equal to 1024.

3.8.3 Card pass phrases

All pass phrases are hashed using the SHA-1 hash mechanism and then combined with a module key to produce the key used to encrypt data on the nShield physical or software token. The pass phrase supplied can be of any length.

The **`ckinittoken`** program imposes a 512-byte limit on the pass phrase.

`C_GetTokenInfo` reports **`_MaxPinLen`** as 256 because some applications may have problems with a larger value.

When **`C_Login`** is called, the pass phrase is used to load private objects protected by that card set on to all modules with cards from that set. Public objects belonging to that set are loaded on to all the modules. **`C_Login`** fails if any logical token fails to load. All cards in a card set must have the same pass phrase.

The functions **`C_SetPIN`**, **`C_InitPIN`**, and **`C_InitToken`** are supported in load-sharing mode only when using softcards. To use these functions in load-sharing mode, you must have created a softcard with the command **`ppmk -n`** before selecting the corresponding slot.PINtPINtToken

The **`C_InitToken`** function is *not* supported for use in non-load-sharing FIPS 140-2 level 3 Security Worlds.

3.9 Functions supported

The following sections list the PKCS #11 functions supported by the nCipher PKCS #11 library. For a list of supported mechanisms, see *Mechanisms* on page 35.

Certain functions are included in PKCS #11 version 2.01 for compatibility with earlier versions only.

3.9.1 General purpose functions

The following functions perform as described in the PKCS #11 specification:

- **`C_Finalize`**
- **`C_GetInfo`**
- **`C_GetFunctionList`**.

3.9.1.1 C_Initialize

If your application uses multiple threads, you must supply such functions as **`CreateMutex`** (as stated in the PKCS #11 specification) in the **`CK_C_INITIALIZE_ARGS`** argument.

3.9.2 Slot and token management functions

The following functions perform as described in the PKCS #11 specification:

- **`C_GetSlotInfo`**
- **`C_GetTokenInfo`**
- **`C_GetMechanismList`**
- **`C_GetMechanismInfo`**.

3.9.2.1 C_GetSlotList

This function returns an array of PKCS #11 slots. Within each module, the slots are in the order:

1. module(s)
2. smart card reader(s)
3. software tokens, if present.

Each module is listed in ascending order by nShield **`ModuleID`**.

ℹ **`C_GetSlotList`** returns an array of handles. You can not make any assumptions about the values of these handles. In particular, these handles are not equivalent to the slot numbers returned by the nCore API command **`GetSlotList.`**

3.9.2.2 C_InitToken

`C_InitToken` sets the card pass phrase to the same value as the PKCS #11 security officer's pass phrase and sets the **`CKF_USER_PIN_INITIALIZED`** flag.

ℹ This function is supported in load-sharing mode only when using softcards. To use **`C_InitToken`** in load-sharing mode, you must have created a softcard with the command **`ppmk -n`** before selecting the corresponding slot.

ℹ The **`C_InitToken`** function is *not* supported for use in non-load-sharing FIPS 140-2 level 3 Security Worlds.

3.9.2.3 C_InitPIN

There is usually no need to call **`C_InitPIN`**, because **`C_InitToken`** sets the card pass phrase.

Because the nCipher PKCS #11 library can only maintain a single pass phrase, **`C_InitPIN`** has the effect of changing the PKCS #11 security officer's pass phrase.

ℹ This function is supported in load-sharing mode only when using softcards. To use **`C_InitPIN`** in load-sharing mode, you must have created a softcard with the command **`ppmk -n`** before selecting the corresponding slot.

3.9.2.4 C_SetPIN

The card pass phrase may be any value.

Because the nCipher PKCS #11 library can only maintain a single pass phrase, **`C_SetPIN`** has the effect of changing the PKCS #11 security officer's pass phrase or, if called in a security officer session, the card pass phrase.

ℹ This function is supported in load-sharing mode only when using softcards. To use **`C_SetPIN`** in load-sharing mode, you must have created a softcard with the command **`ppmk -n`** before selecting the corresponding slot.

3.9.3 Standard session management functions

These functions perform as described in the PKCS #11 specification:

- **`C_OpenSession`**
- **`C_CloseSession`**
- **`C_CloseAllSessions`**
- **`C_GetOperationState`**
- **`C_SetOperationState`**
- **`C_Login`**
- **`C_Logout`**

3.9.4 nShield session management functions

The following are nShield-specific calls for *K/N* card set support:

- **`C_LoginBegin`**
- **`C_LoginNext`**
- **`C_LoginEnd`**
- **`C_GetSessionInfo`**

`ulDeviceError` returns the numeric value of the last status, other than **`Status_OK`**, returned by the module. This value is never cleared. Status values are enumerated in the header file **`messages-args-en.h`** on the nShield Developer's installation media. For descriptions of nShield status codes, see the *nCore API Documentation* (supplied as HTML).

3.9.5 Object management functions

These functions perform as described in the PKCS #11 specification:

- `C_CreateObject`
- `C_CopyObject`
- `C_DestroyObject`
- `C_GetObjectSize`
- `C_GetAttributeValue`
- `C_SetAttributeValue`
- `C_FindObjectsInit`
- `C_FindObjects`
- `C_FindObjectsFinal`

3.9.6 Encryption functions

These functions perform as described in the PKCS #11 specification:

- `C_EncryptInit`
- `C_Encrypt`
- `C_EncryptUpdate`
- `C_EncryptFinal`

3.9.7 Decryption functions

These functions perform as described in the PKCS #11 specification:

- `C_DecryptInit`
- `C_Decrypt`
- `C_DecryptUpdate`
- `C_DecryptFinal`

3.9.8 Message digesting functions

The following functions are performed on the host computer:

- `C_DigestInit`
- `C_Digest`
- `C_DigestUpdate`
- `C_DigestFinal`

3.9.9 Signing and MACing functions

The following functions perform as described in the PKCS #11 specification:

- `C_SignInit`
- `C_Sign`
- `C_SignRecoverInit`
- `C_SignRecover`.

The functions `C_SignUpdate` and `C_SignFinal` are supported for:

- `CKM_SHA1_RSA_PKCS`
- `CKM_MD5_RSA_PKCS`.

3.9.10 Functions for verifying signatures and MACs

The following functions perform as described in the PKCS #11 specification:

- `C_VerifyInit`
- `C_Verify`
- `C_VerifyRecover`
- `C_VerifyRecoverInit`.

The `C_VerifyUpdate` and `C_VerifyFinal` functions are supported for:

- `CKM_SHA1_RSA_PKCS`
- `CKM_MD5_RSA_PKCS`

3.9.11 Dual-purpose cryptographic functions

The following functions perform as described in the PKCS #11 specification:

- `C_DigestEncryptUpdate`
- `C_DecryptDigestUpdate`.

The `C_SignEncryptUpdate` and `C_DecryptVerifyUpdate` functions are supported for:

- `CKM_SHA1_RSA_PKCS`
- `CKM_MD5_RSA_PKCS`

3.9.12 Key-management functions

The following functions perform as described in the PKCS #11 specification:

- `C_GenerateKey`
- `C_GenerateKeyPair`
- `C_WrapKey`
- `C_UnwrapKey`
- `C_DeriveKey`

You can use the `CKNFAST_OVERRIDE_SECURITY_ASSURANCES` environment variable to modify the way that some functions, including key-management functions, are used.

3.9.13 Random number functions

The nShield module has an onboard, hardware random number generator to handle the following random number functions:

- `C_GenerateRandom`
- `C_SeedRandom`

For this reason, it does not use seed values, and the `C_SeedRandom` function returns `CKR_RANDOM_SEED_NOT_SUPPORTED`.

3.9.14 Parallel function management functions

The following functions are supported in the approved fashion by returning the PKCS #11 status `CKR_FUNCTION_NOT_PARALLEL`:

- `C_GetFunctionStatus`
- `C_CancelFunction`

3.9.15 Callback functions

There are no vendor-defined callback functions. Surrender callback functions are never called.

3.9.16 Mechanisms

The following table lists the mechanisms currently supported by the nCipher PKCS #11 library. nCipher also provides vendor-supplied mechanisms, described in *Vendor-defined mechanisms* on page 41.

Some mechanisms may be restricted from use in Security Worlds conforming to FIPS 140-2 Level 3. See the *User Guide* for your HSM for more information.

Mechanism	Functions						
	Encrypt & Decrypt	Sign & Verify	SR & VR	Digest	Gen. Key/Key Pair	Wrap & Unwrap	Derive Key
`CKM_AES_CBC_ENCRYPT_DATA`	—	—	—	—	—	—	Y
`CKM_AES_CBC_PAD`	Y	—	—	—	—	Y	—
`CKM_AES_CBC`	Y	—	—	—	—	Y[5]	—
`CKM_AES_CMAC_GENERAL`	—	Y	—	—	—	—	—
`CKM_AES_CMAC`	—	Y	—	—	—	—	—
`CKM_AES_ECB_ENCRYPT_DATA`	—	—	—	—	—	—	Y
`CKM_AES_ECB`	Y	—	—	—	—	Y[5]	—
`CKM_AES_KEY_GEN`	—	—	—	—	Y	—	—

Mechanism	Functions						
	Encrypt & Decrypt	Sign & Verify	SR & VR	Digest	Gen. Key/Key Pair	Wrap & Unwrap	Derive Key
CKM_AES_KEY_WRAP	—	—	—	—	—	Y	—
CKM_AES_MAC_GENERAL	—	Y	—	—	—	—	—
CKM_AES_MAC	—	Y	—	—	—	—	—
CKM_CONCATENATE_BASE_AND_KEY	—	—	—	—	—	—	Y[8]
CKM_DES_CBC_ENCRYPT_DATA	—	—	—	—	—	—	Y
CKM_DES_CBC_PAD	Y	—	—	—	—	Y	—
CKM_DES_CBC	Y	—	—	—	—	Y	—
CKM_DES_ECB_ENCRYPT_DATA	—	—	—	—	—	—	Y
CKM_DES_ECB	Y	—	—	—	—	Y	—
CKM_DES_KEY_GEN	—	—	—	—	Y	—	—
CKM_DES_MAC_GENERAL	—	Y	—	—	—	—	—
CKM_DES_MAC	—	Y	—	—	—	—	—
CKM_DES2_KEY_GEN	—	—	—	—	Y	—	—
CKM_DES3_CBC_ENCRYPT_DATA	—	—	—	—	—	—	Y
CKM_DES3_CBC_PAD	Y	—	—	—	—	Y	—
CKM_DES3_CBC	Y	—	—	—	—	Y[5]	—
CKM_DES3_ECB_ENCRYPT_DATA	—	—	—	—	—	—	Y
CKM_DES3_ECB	Y	—	—	—	—	Y[5]	—
CKM_DES3_KEY_GEN	—	—	—	—	Y	—	—
CKM_DES3_MAC_GENERAL	—	Y	—	—	—	—	—
CKM_DES3_MAC	—	Y	—	—	—	—	—
CKM_DH_PKCS_DERIVE	—	—	—	—	—	—	Y
CKM_DH_PKCS_KEY_PAIR_GEN	—	—	—	—	Y	—	—
CKM_DSA_KEY_PAIR_GEN	—	—	—	—	Y	—	—
CKM_DSA_PARAMETER_GEN	—	—	—	—	Y	—	—
CKM_DSA_SHA1	—	Y	—	—	—	—	—

Mechanism	Functions						
	Encrypt & Decrypt	Sign & Verify	SR & VR	Digest	Gen. Key/Key Pair	Wrap & Unwrap	Derive Key
CKM_DSA	—	Y[1]	—	—	—	—	—
CKM_EC_EDWARDS_KEY_PAIR_GEN	—	—	—	—	Y[12]	—	—
CKM_EC_KEY_PAIR_GEN	—	—	—	—	Y[10]	—	—
CKM_EC_MONTGOMERY_KEY_PAIR_GEN	—	—	—	—	Y[12]	—	—
CKM_ECDH1_DERIVE	—	—	—	—	—	—	Y[6]
CKM_ECDSA_SHA1	—	Y	—	—	—	—	—
CKM_EDDSA	—	Y[1], [13]	—	—	—	—	—
CKM_ECDSA	—	Y[1]	—	—	—	—	—
CKM_GENERIC_SECRET_KEY_GEN	—	—	—	—	Y	—	—
CKM_MD5_HMAC_GENERAL	—	Y	—	—	—	—	—
CKM_MD5_HMAC	—	Y	—	—	—	—	—
CKM_MD5	—	—	—	Y	—	—	—
CKM_NC_MD5_HMAC_KEY_GEN	—	—	—	—	Y	—	—
CKM_PBE_MD5_DES_CBC	—	—	—	—	Y	—	—
CKM_RIPEMD160	—	—	—	Y	—	—	—
CKM_RSA_9796	—	Y[1]	Y[1]	—	—	—	—
CKM_RSA_PKCS_KEY_PAIR_GEN	—	—	—	—	Y	—	—
CKM_RSA_PKCS_OAEP	Y	—	—	—	—	Y	—
CKM_RSA_PKCS_PSS[9]	Y	Y	—	—	—	—	—
CKM_RSA_PKCS	Y[1]	Y[1]	Y[1]	—	—	Y	—
CKM_RSA_X_509	Y[1]	Y[1]	Y[1]	—	—	X	—
CKM_RSA_X9_31_KEY_PAIR_GEN	—	—	—	—	Y	—	—
CKM_SHA_1_HMAC_GENERAL	—	Y[4]	—	—	—	—	—
CKM_SHA_1_HMAC	—	Y[4]	—	—	—	—	—
CKM_SHA_1	—	—	—	Y	—	—	—

Mechanism	Functions						
	Encrypt & Decrypt	Sign & Verify	SR & VR	Digest	Gen. Key/Key Pair	Wrap & Unwrap	Derive Key
CKM_SHA1_RSA_PKCS_PSS[9]	—	Y	—	—	—	—	—
CKM_SHA1_RSA_PKCS	—	Y	—	—	—	—	—
CKM_SHA224_HMAC_GENERAL	—	Y[4]	—	—	—	—	—
CKM_SHA224_HMAC	—	Y[4]	—	—	—	—	—
CKM_SHA224_RSA_PKCS_PSS[9]	—	Y	—	—	—	—	—
CKM_SHA224	—	—	—	Y	—	—	—
CKM_SHA256_HMAC_GENERAL	—	Y[4]	—	—	—	—	—
CKM_SHA256_HMAC	—	Y[4]	—	—	—	—	—
CKM_SHA256_RSA_PKCS_PSS[9]	—	Y	—	—	—	—	—
CKM_SHA256_RSA_PKCS	—	Y	—	—	—	—	—
CKM_SHA256	—	—	—	Y	—	—	—
CKM_SHA384_HMAC_GENERAL	—	Y[4]	—	—	—	—	—
CKM_SHA384_HMAC	—	Y[4]	—	—	—	—	—
CKM_SHA384_RSA_PKCS_PSS[9]	—	Y	—	—	—	—	—
CKM_SHA384_RSA_PKCS	—	Y	—	—	—	—	—
CKM_SHA384	—	—	—	Y	—	—	—
CKM_SHA512_HMAC_GENERAL	—	Y[4]	—	—	—	—	—
CKM_SHA512_HMAC	—	Y[4]	—	—	—	—	—
CKM_SHA512_RSA_PKCS_PSS[9]	—	Y	—	—	—	—	—
CKM_SHA512_RSA_PKCS	—	Y	—	—	—	—	—
CKM_SHA512	—	—	—	Y	—	—	—
CKM_WRAP_RSA_CRT_COMPONENTS	—	—	—	—	—	Y[11]	—
CKM_XOR_BASE_AND_DATA	—	—	—	—	—	—	Y[3]

The nCipher library supports some mechanisms that are defined in versions of the PKCS #11 standard later than 2.01, although the nCipher library does not fully support versions of the PKCS #11 standard later than 2.01. In the table above:

- Empty cells indicate mechanisms that are not supported by the PKCS #11 standard.
- The entry **Y** indicates that a mechanism is supported by the nCipher PKCS #11 library.
- The entry **X** indicates that a mechanism is not supported by the nCipher PKCS #11 library.

In the table above, annotations with the following numbers indicate:

1. Single-part operations only.
2. This mechanism uses the eight octets following the key as the initializing vector as specified in PKCS#5 v2.
3. The base key and the derived key are restricted to **DES**, **DES3**, **CAST5** or **Generic**, though they may be of different types.
4. This mechanism depends on the vendor-defined key generation mechanism **CKM_NC_SHA_1_HMAC_KEY_GEN**, **CKM_NC_SHA224_HMAC_KEY_GEN**, **CKM_NC_SHA256_HMAC_KEY_GEN**, **CKM_NC_SHA384_HMAC_KEY_GEN**, or **CKM_NC_SHA512_HMAC_KEY_GEN**. For more information, see *Vendor-defined mechanisms* on page 41.
5. Wrap secret keys only (private key wrapping must use **CBC_PAD**).
6. The **CKM_ECDH1_DERIVE** mechanism is supported. However, the mechanism only takes a **CK_ECDH1_DERIVE_PARAMS** struct in which **CK_EC_KDF_TYPE** is **CKD_NULL**, **CKD_SHA1_KDF**, **CKD_SHA224_KDF**, **CKD_SHA256_KDF**, **CKD_SHA384_KDF**, or **CKD_SHA512_KDF**. For more information on **CK_ECDH1_DERIVE_PARAMS**, see the PKCS #11 standard.

   For the **pPublicData*** parameter, a raw octet string value (as defined in section A.5.2 of ANSI X9.62) and DER-encoded ECPoint value (as defined in section E.6 of ANSI X9.62 or, in the case of **CKK_EC_MONTGOMERY**, RFC 7748) are now accepted.

7. Before you can create a key for use with the derive mechanism **CKM_CONCATENATE_BASE_AND_KEY**, you must first specify the **CKA_ALLOWED_MECHANISMS** attribute in the template with the **CKM_CONCATENATE_BASE_AND_KEY** set. Specifying the **CKA_ALLOWED_MECHANISMS** in the template enables the setting of the nCore level ACL, which enables the key in this derive key operation. For more information about:
   - the Security Assurance Mechanisms (SAMs) on the **CKM_CONCATENATE_BASE_AND_KEY** mechanism, see *PKCS #11* on page 19
   - the **CKA_ALLOWED_MECHANISMS** attribute, see *Attributes* on page 49.

8. The **hashAlg** and the **mgf** that are specified by the **CK_RSA_PKCS_PSS_PARAMS** must have the same SHA hash size. If they do not have the same hash size, then the signing or verify fails with a return value of **CKR_MECHANISM_PARAM_INVALID**.

   The **sLen** value is expected to be the length of the message hash. If this is not the case, then the signing or verify again fails with a return value of **CKR_MECHANISM_PARAM_INVALID**. The Security World Software implementation of **RSA_PKCS_PSS** salt lengths are as follows:

Mechanism	Salt-length
SHA-1	160-bit
SHA-224	224-bit
SHA-256	256-bit
SHA-384	384-bit
SHA-512	512-bit

9. The **hashAlg** and the **mgf** that are specified by the **CK_RSA_PKCS_OEAP_PARAMS** must have the same SHA hash size. If they do not have the same hash size, then the signing or verify fails with a return value of **CKR_MECHANISM_PARAM_INVALID**.

   It is possible to specify a byte array using a data source if **CKZ_DATA_SPECIFIED** is set. If **CKZ_DATA_SPECIFIED** is not present, then **pSourceData** and **pSourceDatalen** are ignored. It is not a requirement to have source set, and the value can be zero.

10. For elliptic curve key pairs: when generating a key pair using **C_GenerateKeyPair()**, you may specify either **CKA_DERIVE** or **CKA_SIGN** but not both. This means that your **CKK_EC** key can only be used for either sign/verify or derive operations. If both types are included in the template, generation fails with **CKR_TEMPLATE_INCONSISTENT**. If nothing is specified in the template, then the default is sign/verify.

    Key generation does calculate its own curves but, as shown in the PKCS #11 standard, takes the **CKA_PARAMS**, which contains the curve information (similar to that of a discrete logarithm group in the generation of a DSA key pair). **CKA_EC_PARAMS** is a Byte array which is DER-encoded of an ANSI X9.62 Parameters value. It can take both named curves and custom curves.
    The following PKCS #11-specific flags describe which curves are supported:

    - **CKF_EC_P**: prime curve supported
    - **CKF_EC_2M**: binary curve supported
    - **CKF_EC_PARAMETERS**: supplying your own custom parameters is supported
    - **CKF_EC_NAMECURVE**: supplying a named curve is supported
    - **CKF_EC_UNCOMPRESS**: supports uncompressed form only, compressed form not supported.

11. Wrap only.

12. **CKA_EC_PARAMS** is a DER-encoded PrintableString **curve25519**.

13. Only the **Ed25519ph** signature scheme is supported, requiring **CK_EDDSA_PARAMS** to have the following set:
    - **phFlag** to **CK_TRUE**
    - **ulContextDataLen** to **0**.

3.9.17 Vendor-defined mechanisms

The following vendor-defined mechanisms are also available. The numeric values of vendor-defined key types and mechanisms can be found in the supplied **pkcs11extra.h** header file.

ℹ Some mechanisms may be restricted from use in Security Worlds conforming to FIPS 140-2 Level 3. See the *User Guide* for your HSM for more information.

3.9.17.1 CKM_WRAP_RSA_CRT_COMPONENTS

This wrapping mechanism uses a **pMechanism->pParameter** argument that is itself a **CK_MECHANISM_PTR** appropriate for the underlying encryption mechanism. The wrapping mechanism takes a pointer to a PKCS #11 template as its **pWrappedKey** argument.

The **CK_ATTRIBUTE_PTR** template is allocated by the calling application. The template is filled in by the calling application with the attribute types (**CKA_PRIME_1**, **CKA_PRIME_2**, **CKA_EXPONENT_1**, **CKA_EXPONENT_2**, **CKA_COEFFICIENT**), and the lengths of the value buffers, which are also allocated by the application. The **pulWrappedKeyLen** argument contains the length in bytes of the template, which is **(5 * sizeof(CK_ATTRIBUTE_PTR))**.

The usual method of calling **C_WrapKey** is with a **NULL** buffer to determine its output length. This is not available because **C_WrapKey** cannot specify the multiple levels of allocation required. If any part of this structure has an inappropriate size, the mechanism fails with a **CKR_WRAPPED_KEY_LEN_RANGE** error.

3.9.17.2 CKM_SEED_ECB_ENCRYPT_DATA & CKM_SEED_CBC_ENCRYPT_DATA

This mechanism derives a secret key by encrypting plain data with the specified secret base key. This mechanism takes as a parameter a **CK_KEY_DERIVATION_STRING_DATA** structure, which specifies the length and value of the data to be encrypted by using the base key to derive another key.

If no length or key type is provided in the template, the key produced by this mechanism is a generic secret key. Its length is equal to the length of the data.

If a length, but no key type, is provided in the template, the key produced by this mechanism is a generic secret key of the specified length.

If a key type, but no length, is provided in the template, the key type must have a well-defined length. If the length is well defined, the key produced by this mechanism is of the type specified in the template. If the length is not well defined, a **CKR_TEMPLATE_INCOMPLETE** error is returned.

If both a key type and a length are provided in the template, the length must be compatible with that key type, and **CKR_TEMPLATE_INCONSISTENT** is returned if it is not.

The key produced by the **CKM_SEED_ECB_ENCRYPT_DATA** or **CKM_SEED_CBC_ENCRYPT_DATA** mechanisms is of the specified type and length.

3.9.17.3 CKM_CAC_TK_DERIVATION

This mechanism uses **C_GenerateKey** to perform an **Import** operation using a Transport Key Component.

The mechanism accepts a template that contains three Transport Key Components (TKCs) with following attribute types:

- **CKA_TKC1**
- **CKA_TKC2**
- **CKA_TKC3**.

These attributes are all in the **CKA_VENDOR_DEFINED** range.

Each TKC should be the same length as the key being created. TKCs used for DES, DES2, or DES3 keys must have odd parity. The mechanism checks for odd parity and returns **CKR_ATTRIBUTE_VALUE_INVALID** if it is not found.

The new key is constructed by an XOR of the three TKC components on the module.

Although using **C_GenerateKey** creates a key with a known value rather than generating a new one, it is used because **C_CreateObject** does not accept a mechanism parameter.

CKA_LOCAL, **CKA_ALWAYS_SENSITIVE**, and **CKA_NEVER_EXTRACTABLE** are set to **FALSE**, as they would for a key imported with **C_CreateObject**. This reflects the fact that the key was not generated locally.

An example of the use of **CKM_CAC_TK_DERIVATION** is shown here:

```
CK_OBJECT_CLASS class_secret = CKO_SECRET_KEY;
        CK_KEY_TYPE key_type_des2 = CKK_DES2;
        CK_MECHANISM mech = { CKM_CAC_TK_DERIVATION, NULL_PTR, 0 };
        CK_BYTE TKC1[16] = { ... };
        CK_BYTE TKC2[16] = { ... };
        CK_BYTE TKC3[16] = { ... };
        CK_OBJECT_HANDLE kHey;
        CK_ATTRIBUTE pTemplate[] = {
                { CKA_CLASS, &class_secret, sizeof(class_secret) },
                { CKA_KEY_TYPE, &key_type_des2, sizeof(key_type_des2) },
                { CKA_TKC1, TKC1, sizeof(TKC1) },
                { CKA_TKC2, TKC1, sizeof(TKC2) },
                { CKA_TKC3, TKC1, sizeof(TKC3) },
                { CKA_ENCRYPT, &true, sizeof(true) },
        ....
        };

        rv = C_GenerateKey(hSession, &mechanism, pTemplate,
                (sizeof(pTemplate)/sizeof((pTemplate)[0])), &hKey);
```

3.9.17.4 CKM_SHA*_HMAC and CKM_SHA*_HMAC_GENERAL

This version of the library supports the PKCS #11 standard mechanisms for SHA-1 and SHA-2 HMAC as defined in PKCS #11 standard version 2.30:

- **CKM_SHA_1_HMAC**
- **CKM_SHA_1_HMAC_GENERAL**

- **CKM_SHA224_HMAC**
- **CKM_SHA224_HMAC_GENERAL**
- **CKM_SHA256_HMAC**
- **CKM_SHA256_HMAC_GENERAL**
- **CKM_SHA384_HMAC**
- **CKM_SHA384_HMAC_GENERAL**
- **CKM_SHA512_HMAC**
- **CKM_SHA512_HMAC_GENERAL**

For security reasons, the Security World Software supports these mechanisms only with their own specific key type. Thus, you can only use an HMAC key with the HMAC algorithm and not with other algorithms.

The PKCS #11 standard does not provide an appropriate key type. Therefore, the vendor-defined key types **CKK_SHA_1_HMAC**, **CKK_SHA224_HMAC**, **CKK_SHA256_HMAC**, **CKK_SHA384_HMAC**, and **CKK_SHA512_HMAC**, are provided for use with these SHA-1 and SHA-2 HMAC mechanisms. To generate the key, use the appropriate vendor-defined key generation mechanism (which does not take any mechanism parameters):

- **CKM_NC_MD5_HMAC_KEY_GEN**
- **CKM_NC_SHA_1_HMAC_KEY_GEN**
- **CKM_NC_SHA224_HMAC_KEY_GEN**
- **CKM_NC_SHA256_HMAC_KEY_GEN**
- **CKM_NC_SHA384_HMAC_KEY_GEN**
- **CKM_NC_SHA512_HMAC_KEY_GEN**

3.9.17.5 CKM_NC_ECKDF_HYPERLEDGER

This version of the library supports the vendor-defined **CKM_NC_ECKDF_HYPERLEDGER** mechanism. This key derivation function is used in the user/client enrolment process of a hyperledger system to generate transaction certificates by using the enrolment certificate as one of the inputs to the key derivation.

The parameters for the mechanism are defined in the following structure:

```
typedef struct CK_ECKDF_HYPERLEDGERCLIENT_PARAMS {
    CK_OBJECT_HANDLE hKeyDF_Key;
    CK_MECHANISM_TYPE HMACMechType;
    CK_MECHANISM_TYPE TCertEncMechType;
    CK_ULONG ulEksize;
    CK_BYTE_PTR pEncTCertData;
    CK_ULONG ulEvsize;
    CK_ULONG ulEndian;
} CK_ECKDF_HYPERLEDGERCLIENT_PARAMS
```

Where:

- **`hKeyDF_key`** is **KeyDF_Key**
- **`HMACMechType`** is **Hmac**
- **`TCertEncMechType`** is **Decrypt_Mech**
- **`ulEksize`** is **Eksize**
- **`pEncTCertData`** is a pointer to encrypted data containing TCertIndex together with padding and IV
- **`ulEvsize`** is **Evsize**
- **`ulEndian`** is **Big_Endian**

The function is then called as follows:

```
C_DeriveKey(
    hSession,
    &mechanism_hyperledger,
    EnrollPriv_Key,
    TCertPriv_Key_template,
    NUM(TCertPriv_Key_template,
    &TCertPriv_Key);
```

A **Template_Key** will be used to supply key attributes for the resulting derived key. The derived key can then be used in the normal way.

Derived keys can be exported and used outside the HSM only if the template key was created with attributes which allow export of its derived keys.

3.9.17.6 CKM_HAS160

This version of the library supports the vendor-defined **`CKM_HAS160`** hash (digest) mechanism for use with the **`CKM_KCDSA`** mechanism. For more information, see *Mechanisms for KISAAlgorithms* on page 46.

3.9.17.7 CKM_PUBLIC_FROM_PRIVATE

`CKM_PUBLIC_FROM_PRIVATE` is a derive key mechanism that enables the creation of a corresponding public key from a private key. The mechanism also fills in the public parts of the private key, where this has not occurred.

`CKM_PUBLIC_FROM_PRIVATE` is an nShield specific nCore mechanism. The **`C_Derive`** function takes the object handle of the private key and the public key attribute template. The creation of the key is based on the template but also checked against the attributes of the private key to ensure the attributes are correct and match those of the corresponding key. If an operation that is not allowed or is not set by the private key is detected, then **`CKR_TEMPLATE_INCONSISTANT`** is returned.

Before you can use this mechanism, the HSM must already contain the private key. You must use **`C_CreateObject`**, **`C_UnWrapKey`**, or **`C_GenerateKeyPair`** to import or generate the private key.

If you use **`C_GenerateKeyPair`**, you always generate a public key at the same time as the private key. Some applications delete public keys once a certificate is imported, but in the case of both **C_GenerateKeyPair** and **C_CreateObject** you can use either the **CKM_PUBLIC_FROM_PRIVATE** mechanism or the **C_GetAttributeValue** to recreate a deleted public key.

3.9.17.8 CKM_NC_AES_CMAC

CKM_NC_AES_CMAC is based on the **Mech_RijndaelCMAC** nCore level mechanism, a message authentication code operation that is used with both **C_Sign** and **C_SignUpdate**, and the corresponding **C_Verify** and **C_VerifyUpdate** functions.

In a similar way to other AES MAC mechanisms, **CKM_NC_AES_CMAC** takes a plaintext type of any length of bytes, and returns a **M_Mech_Generic128MAC_Cipher** standard byte block. **CKM_NC_AES_CMAC** is a standard FIPS 140-2 Level 3 approved mechanism, and is only usable with **CKK_AES** key types.

CKM_NC_AES_CMAC has a **CK_MAC_GENERAL_PARAMS** which is the length of the MAC returned (sometimes called a tag length). If this is not specified, the signing operation fails with a return value of **CKR_MECHANISM_PARAM_INVALID**.

3.9.17.9 CKM_NC_AES_CMAC_KEY_DERIVATION and CKM_NC_AES_CMAC_KEY_DERIVATION_SCP03

This mechanism derives a secret key by validating parameters with the specified 128-bit, 192-bit, or 256-bit secret base AES key. This mechanism takes as a parameter a **CK_NC_AES_CMAC_KEY_DERIVATION_PARAMS** structure, which specifies the length and type of the resulting derived key.

CKM_NC_AES_CMAC_KEY_DERIVATION_SCP03 is a variant of **CKM_NC_AES_CMAC_KEY_DERIVATION**: it reorders the arguments in the **CK_NC_AES_CMAC_KEY_DERIVATION_PARAMS** according to payment specification **SCP03**, but is otherwise identical.

The standard key attribute behavior with **sensitive** and **extractable** attributes is applied to the resulting key as defined in PKCS #11 standard version 2.20 and later. The key type and template declaration is based on the PKCS #11 standard key declaration for derive key mechanisms.

If no length or key type is provided in the template, the key produced by this mechanism is a generic secret key. Its length is equal to the length of the data.

If a length, but no key type, is provided in the template, the key produced by this mechanism is a generic secret key of the specified length.

If a key type, but no length, is provided in the template, the key type must have a well-defined length. If the length is well defined, the key produced by this mechanism is of the type specified in the template. If the length is not well defined, a **CKR_TEMPLATE_INCOMPLETE** error is returned.

If both a key type and a length are provided in the template, the length must be compatible with that key type, and **CKR_TEMPLATE_INCONSISTENT** is returned if it is not.

The key produced by the **CKM_NC_AES_CMAC_KEY_DERIVATION** mechanism is of the specified type and length. If a DES, DES2, DES3, or CDMF key is derived with this mechanism, the parity bits of the key are set properly. If the requested type of key requires more bytes than are available by concatenating the original key values, an error is generated.

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

Attribute	If the attributes for the *original keys* are...	The attribute for the *derived key* is...
CKA_SENSITIVE	CK_TRUE for either one	CK_TRUE
CKA_EXTRACTABLE	CK_FALSE for either one	CK_FALSE
CKA_ALWAYS_SENSITIVE	CK_TRUE for both	CK_TRUE
CKA_NEVER_EXTRACTABLE	CK_TRUE for both	CK_TRUE

CK_NC_AES_CMAC_KEY_DERIVATION_PARAMS

```
typedef struct CK_NC_AES_CMAC_KEY_DERIVATION_PARAMS {
    CK_ULONG ulContextLen;
    CK_BYTE_PTR pContext;
    CK_ULONG ulLabelLen;
    CK_BYTE_PTR pLabel;
  } CK_NC_AES_CMAC_KEY_DERIVATION_PARAMS;
```

The fields of the structure have the following meanings:

Argument	Meaning
ulContextLen	Context data: the length in bytes.
pContext	Some data info context data (bytes to be CMAC'd). **`ulContextLen`** must be zero if **`pContext`** is not provided. Having **`pContext`** as NULL will result in the same predictable key each time not additional data to add to the mix when carrying out the CMAC.
ulLabelLen	The length in bytes of the other party EC public key
pLabel	Key derivation label data: a pointer to the other label to identify new key. **`ulLabelLen`** must be zero if the **`pLabel`** is not provided.

3.9.17.10 CKM_COMPOSITE_EMV_T_ARQC, CKM_WATCHWORD_PIN1 and CKM_WATCHWORD_PIN2

These mechanisms allow the module to act as a SafeSign Cryptomodule (SSCM). To obtain support for your product, visit: https://help.ncipher.com.

3.9.18 Mechanisms for KISAAlgorithms

If you are using version 1.20 or greater and you have enabled the **`KISAAlgorithms`** feature, you can use the following mechanisms through the standard PKCS #11 API calls.

3.9.18.1 KCDSA keys

The **`CKM_KCDSA`** mechanism is a plain general signing mechanism that allows you to use a **`CKK_KCDSA`** key with any length of plain text or pre-hashed message. It can be used with the standard single and multipart **`C_Sign`** and **`C_Verify`** update functions.

The **CKM_KCDSA** mechanism takes a **CK_KCDSA_PARAMS** structure that states which hashing mechanism to use and whether or not the hashing has already been performed:

```
typedef struct CK_KCDSA_PARAMS {
        CK_MECHANISM_PTR digestMechanism;
        CK_BBOOL dataIsHashed;
}
```

The following digest mechanisms are available for use with the digestMechanism:

- **CKM_SHA_1**
- **CKM_HAS160**
- **CKM_RIPEMD160**

The **dataIsHashed** flag can be set to one of the following values:

- **1** when the message has been pre-hashed (pre-digested)
- **0** when the message is in plain text.

The **CK_KCDSA_PARAMS** structure is then passed in to the mechanism structure.

3.9.18.2 Pre-hashing

If you want to provide a pre-hashed message to the **C_Sign()** or **C_Verify()** functions using the **CKM_KCDSA** mechanism, the hash must be the value of $h(z||m)$ where:

- h is the hash function defined by the mechanism
- z is the bottom 512 bits of the public key, with the most significant byte first
- m is the message that is to be signed or verified.

The hash consists of the bottom 512 bits of the public key (most significant byte first), with the message added after this.

If the hash is not formatted as described when signing, then incorrect signatures are generated. If the hash is not formatted as described when verifying, then invalid signatures can be accepted and valid signatures can be rejected.

3.9.18.3 CKM_KCDSA_SHA1, CKM_KCDSA_HAS160, CKM_KCDSA_RIPEMD160

These older mechanisms sign and verify using a **CKK_KCDSA** key. They now work with the **C_Sign** and **C_Update** functions, though they do not take the **CK_KCDSA_PARAMS** structure or pre-hashed messages. These mechanisms can be used for single or multipart signing and are not restricted as to message size.

3.9.18.4 CKM_KCDSA_KEY_PAIR-GEN

This mechanism generates a **CKK_KCDSA** key pair similar to that of DSA. You can supply in the template a discrete log group that consists of the **CKA_PRIME**, **CKA_SUBPRIME**, and **CKA_BASE** attributes. In addition, you must supply **CKA_PRIME_BITS**, with a value between 1024 and 2048, and **CKA_SUBPRIME_BITS**, which must have a value of 160. If you supply **CKA_PRIME_BITS** and **CKA_SUBPRIME_BITS** without a discrete log group, the module generates the group. **CKR_TEMPLATE_INCOMPLETE** is returned if **CKA_PRIME_BITS** and **CKA_SUBPRIME_BITS** are not supplied.

CKA_PRIME_BITS must have the same length as the prime and **CKA_SUBPRIME-BITS** must have the same length as the subprime if the discrete log group is also supplied. If either are different, PKCS #11 returns **CKR_TEMPLATE_INCONSISTENT**.

You can use the **C_GenerateKeyPair** function to generate a key pair. If you supply one or more parts of the discrete log group in the template, the PKCS #11 library assumes that you want to supply a specific discrete log group. **CKR_TEMPLATE_INCOMPLETE** is returned if not all parts are supplied. If you want the module to calculate a discrete log group for you, ensure that there are no discrete log group attributes present in the template.

A **CKK_KCDSA** private key has two value attributes, **CKA_PUBLIC_VALUE** and **CKA_PRIVATE_VALUE**. This is in contrast to DSA keys, where the private key has only the attribute **CKA_VALUE**, the private value. The public key in each case contains only the public value.

The standard key-pair attributes common to all key pairs apply. Their values are the same as those for DSA pairs unless specified differently in this section.

3.9.18.5 CKM_KCDSA_PARAMETER_GEN

For information about DOMAIN Objects, read the PKCS #11 specification v2.11.

Use this mechanism to create a **CKO_DOMAIN_PARAMETERS** object. This is referred to as a **KCDSAComm** key in the nCore interface.

Use **C_GenerateKey** to generate a new discrete log group and initialization values. The initialization values consist of a counter (**CKA_COUNTER**) and a hash (**CKA_SEED**) that is the same length as **CKA_PRIME_BITS**, which must have a value of 160. The **CKA_SEED** must be the same size as **CKA_SUBPRIME_BITS**. If this not the case, the PKCS #11 library returns **CKR_DOMAIN_PARAMS_INVALID**.

Optionally, you can supply the initialization values. If you supply the initialization values with **CKA_PRIME_BITS** and **CKA_SUBPRIME_BITS**, you can reproduce a discrete log group generated elsewhere. This allows you to verify that the discrete log group used in key pairs is correct. If the initialization values are not present in the template, a new discrete log group and corresponding initialization values are generated. These initialization values can be used to reproduce the discrete log group that has just been generated. The newly generated discrete log group can then be used in a PKCS #11 template to generate a **CKK_KCDSA** key using **C_Generate_Key_Pair**. **DOMAIN** keys can also be imported using the **C_CreateObject** call.

3.9.18.6 SEED secret keys:

3.9.18.7 CKM_SEED_KEY_GEN

This mechanism generates a 128-bit SEED key. The standard secret key attributes are required, except that no length is required since this a fixed length key type similar to DES3. Normal return values apply when generating a **CKK_SEED** type key.

3.9.18.8 CKM_SEED_ECB CKM_SEED_CBC CKM_SEED_CBC_PAD

These mechanisms are the standard mechanisms to be used when encrypting and decrypting or wrapping with a **CKK_SEED** key. A **CKK_SEED** key can be used to wrap or unwrap both secret keys and private keys. A **CKK_KCDSA** key cannot be wrapped by any key type.

The **CKM_SEED_ECB** mechanism wraps only secret keys of exact multiples of the **CKK_SEED** block size (16) in ECB mode. The **CKM_SEED_CBC_PAD** key wraps the same keys in CBC mode.

The **CKM_SEED_CBC_PAD** key wraps keys of variable block size. It is the only mechanism available to wrap private keys.

A **CKK_SEED** key can be used to encrypt and decrypt with both single and multipart methods using the standard PKCS #11 API. The plain text size for multipart cryptographic function must be a multiple of the block size.

3.9.18.9 CKM_SEED_MAC CKM_SEED_MAC_GENERAL

These mechanisms perform both signing and verification. They can be used with both single and multipart signing or verification using the standard PKCS #11 API. Message size does not matter for either single or multipart signing and verification.

For information on the padding schemes used by these mechanisms, see *PKCS #11* on page 19.

3.9.18.10 CKM_HAS160

CKM_HAS160 is a basic hashing algorithm. The hashing is done on the host machine. This algorithm can be used by means of the standard digest function calls of the PKCS #11 API.

3.9.19 Attributes

The following sections describe how PCKS #11 attributes map to the Access Control List (ACL) given to the key by the nCore API. nCore API ACLs are described in the *nCore API Documentation* (supplied as HTML).

3.9.19.1 CKA_SENSITIVE

In a non-FIPS 140-2 level 3 world, **CKA_SENSITIVE=FALSE** creates a key with an ACL that includes **ExportAsPlain**. Keys are exported using **DeriveMech_EncryptMarshalled** even in a non-FIPS 140-2 level 3 world. The presence of the **ExportAsPlain** permission makes the status of the key clear when a non-FIPS 140-2 level 3 ACL is viewed using **GetACL**.

CKA_SENSITIVE=FALSE always creates a key with an ACL that includes **DeriveKey** with **DeriveRole_BaseKey** and **DeriveMech_EncryptMarshalled**.

3.9.19.2 CKA_PRIVATE

If **CKA_PRIVATE** is set to **TRUE**, keys are protected by the logical token of the OCS. If it is set to **FALSE**, public keys are protected by a well-known module key, and other keys and objects are protected by the Security World module key.

You must set **CKA_PRIVATE** to:

- **FALSE** for public keys
- **TRUE** for non-extractable keys on card slots.

3.9.19.3 CKA_EXTRACTABLE

CKA_EXTRACTABLE creates a key with an ACL including **DeriveKey** permission with **DeriveRole_BaseKey** and **DeriveMech_RawEncrypt**, as well as with **DeriveMech_PKCS8Encrypt** and **DeriveMech_RSAComponents** for private keys. IGN_RECOVER

3.9.19.4 CKA_ENCRYPT, CKA_DECRYPT, CKA_SIGN, CKA_VERIFY

These attributes create a key with ACL including **Encrypt**, **Decrypt**, **Sign**, or **Verify** permission.

3.9.19.5 CKA_WRAP, CKA_UNWRAP

CKA_WRAP creates a key with an ACL including **DeriveKey** permission with **DeriveRole_WrapKey**, **DeriveMech_RawEncrypt**, as well as with **DeriveMech_PKCS8Encrypt** and **DeriveMech_RSAComponents** for secret keys.

CKA_UNWRAP creates a key with an ACL including **DeriveKey** permission with **DeriveRole_WrapKey** and **DeriveMech_RawDecrypt.**

There is no unwrap mechanism that corresponds to **DeriveMech_RSAComponents**.

3.9.19.6 CKA_SIGN_RECOVER

C_SignRecover checks **CKA_SIGN_RECOVER** but is otherwise identical to **C_Sign**. Setting **CKA_SIGN_RECOVER** creates a key with an ACL that includes **Sign** permission.

3.9.19.7 ERIFY_RECOVERCKA_VERIFY_RECOVER

Setting **CKA_VERIFY_RECOVER** creates a public key with an ACL including **Encrypt** permission.

3.9.19.8 CKA_DERIVE

For Diffie-Hellman private keys, **CKA_DERIVE** creates a key with **Decrypt** permissions.

For secret keys, **CKA_DERIVE** creates a key with an ACL that includes **DeriveRole_BaseKey** with one of **DeriveMech_DESsplitXOR**, **DeriveMech_DES2splitXOR**, **DeriveMech_DES3splitXOR**, **DeriveMech_RandsplitXOR**, or **DeriveMech_CASTsplitXOR** as appropriate if the key is extractable, because this permission would effectively allow the key to be extracted. The ACL includes **DeriveMech_RawEncrypt** whether or not the key is extractable.

3.9.19.9 CKA_ALLOWED_MECHANISMS

CKA_ALLOWED_MECHANISMS is available as a full attribute array for all key types. The number of mechanisms in the array is the **ulValueLen** component of the attribute divided by the size of **CK_MECHANISM_TYPE**.

The **CKA_ALLOWED_MECHANISMS** attribute is set when generating, creating and unwrapping keys. You must set **CKA_ALLOWED_MECHANISMS** with the **CKM_CONCATENATE_BASE_AND_KEY** mechanism when generating or creating both of the keys that are used in the **`C_DeriveKey`** operation with the **`CKM_CONCATENATE_BASE_AND_KEY`** mechanism. If **`CKA_ALLOWED_MECHANISMS`** is not set at creation time then the correct **`ConcatenateBytes`** ACL is not set for the keys.

When **`CKM_CONCATENATE_BASE_AND_KEY`** is used with **`C_DeriveKey`**, **`CKA_ALLOWED_MECHANISMS`** is checked. If **`CKM_CONCATENATE_BASE_AND_KEY`** is not present, then an error occurs and a value of **`CKR_MECHANISM_INVALID`** is returned.

`CKA_ALLOWED_MECHANISMS` is an optional attribute and does not have to be set for any other operations. However, if **`CKA_ALLOWED_MECHANISMS`** is set, then the attribute is checked to see if the mechanism you want to use is in the list of allowed mechanisms. If the mechanism is not present, then an error occurs and a value of **`CKR_MECHANISM_INVALID`** is returned.

3.9.19.10 CKA_MODIFIABLE

`CKA_MODIFIABLE` only restricts access through the PKCS #11 API: all PKCS #11 keys have ACLs that include the **`ReduceACL`** permission.

3.9.19.11 CKA_TOKEN

Token objects are saved as key blobs. Session objects only ever exist on the module.

3.9.19.12 CKA_START_DATE, CKA_END_DATE

These attributes are ignored, and the PKCS #11 standard states that these attributes do not restrict key usage.

3.9.19.13 RSA key values

`CKA_PRIVATE_EXPONENT` is not used when importing an RSA private key using **`C_CreateObject`**. However, it must be in the template, since the PKCS #11 standard requires it. All the other values are required.

The nCore API allows use of a default public exponent, but the PKCS #11 standard requires **`CKA_PUBLIC_EXPONENT`**.

Except for very small keys, the nCipher default is 65537, which as a PKCS #11 big integer is **`CK_BYTEpublic_exponent[ ] = { 1, 0, 1 };`**

3.9.19.14 DSA key values

If **`CKA_PRIME`** is 1024 bits or less, then the **`KeyType_DSAPrivate_GenParams_flags_Strict`** flag is used, because it enforces a 1024 bit limit.

The implementation allows larger values of **`CKA_PRIME`**, but in those cases the **`KeyType_DSAPrivate_GenParams_flags_Strict`** flag is not used.

3.9.19.15 Vendor specific error codes

Security World Software defines the following vendor specific error codes:

`CKR_FIPS_TOKEN_NOT_PRESENT`

This error code indicates that an Operator Card is required even though the card slot is not in use.

`CKR_FIPS_MECHANISM_INVALID`

This error code indicates that the current mechanism is not allowed in FIPS 140-2 level 3 mode.

`CKR_FIPS_FUNCTION_NOT_SUPPORTED`

This error code indicates that the function is not supported in FIPS 140-2 level 3 mode (although it is supported in FIPS 140-2 level 2 mode).

3.9.20 Utilities

This section describes command-line utilities nCipher provides as aids to developers.

3.9.20.1 ckdes3gen

```
ckdes3.gen.exe [p|--pin-for-testing=passphrase] | [n|-nopin]
```

This utility is an example of Triple DES key generation using the nCipher PKCS #11 library. The utility generates the DES3 key as a private object that can be used both to encrypt and decrypt.

By default the utility prompts for a pass phrase. You can supply a pass phrase on the command line with the **`--pin-for-testing`** option, or suppress the pass phrase request with the **`--nopin`** option. The pass phrase is displayed in the clear on the command line, so this option is appropriate only for testing.

3.9.20.2 ckinfo

```
ckinfo.exe [r|--repeat-count=COUNT]
```

This utility displays **`C_GetInfo`**, **`C_GetSlotInfo`** and **`C_GetTokenInfo`** results. You can specify a number of repetitions of the command with **`--repeat-count=`***COUNT*. The default is **`1`**.

3.9.20.3 cklist

```
cklist.exe [-p|--pin-for-testing=passphrase] [-n|-nopin]
```

This utility lists some details of objects on all slots. It lists public and private objects if invoked with a pass phrase argument and public objects only if invoked without a pass phrase argument.

It does not output any potentially sensitive attributes, even if the object has **`CKA_SENSITIVE`** set to **`FALSE`**.

By default the utility prompts for a pass phrase. You can supply a pass phrase on the command line with the **`--pin-for-testing option`**, or suppress the pass phrase request with the **`--nopin`** option. The pass phrase is displayed in the clear on the command line, so this option is appropriate only for testing.

3.9.20.4 ckmechinfo

```
ckmechinfo.exe
```

The utility displays **`C_GetMechanismInfo`** results for each mechanism returned by **`C_GetMechanismList`**.

3.9.20.5 ckrsagen

```
ckrsagen.exe [-p|--pin-for-testing=passphrase] | [-n|-nopin]
```

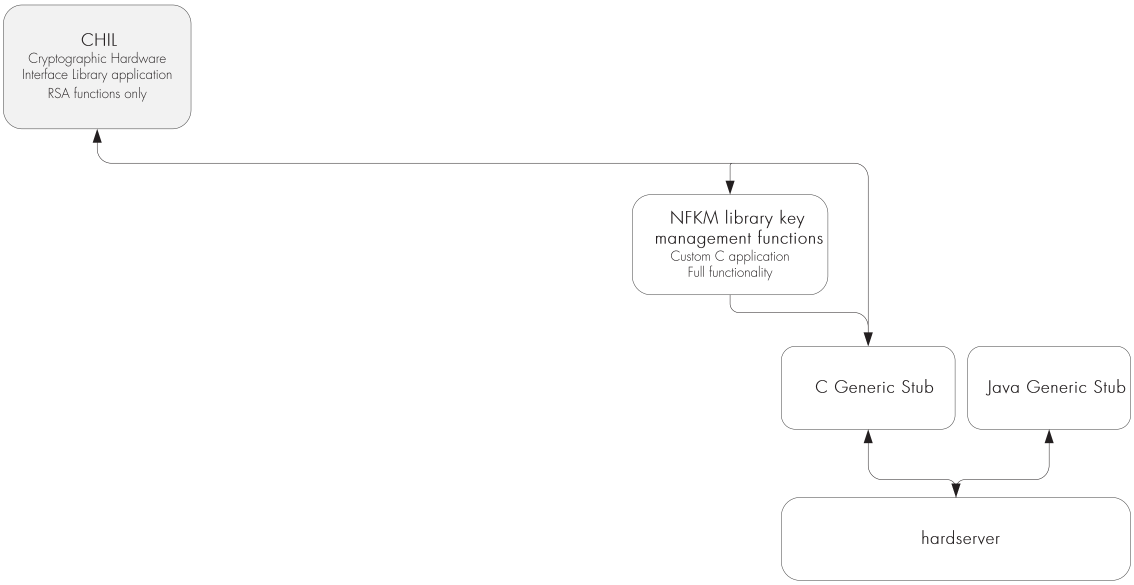
The **`ckrsagen`** utility is an example of RSA key pair generation using the nCipher PKCS #11 library. This is intended as a programmer's example only and not for general use. Use the key generation routines within your PKCS #11 application.

By default the utility prompts for a pass phrase. You can supply a pass phrase on the command line with the **`--pin-for-testing`** option, or suppress the pass phrase request with the **`--nopin`** option. The pass phrase is displayed in the clear on the command line, so this option is appropriate only for testing.

4 CHIL

The Cryptographic Hardware Interface Library (CHIL) is an API for cryptographic modules that perform modulo exponentiation, RSA cryptography, Diffie-Hellman key exchange and DSA for signature creation. RSA encryption can be performed on keys provided in the command or with keys protected by the cryptographic module.

Figure 3. CHIL architecture



The CHIL does not provide a user interface. Instead, it defines a number of callback functions. It is up to the application that is calling the library to implement the user interface required when a callback is made and to pass the input from the user back to the library.

The CHIL is supplied as a library that exports entry point(s) defined in the file **`hwcryptohook.h`**. This set of entry points provides a multithreaded, synchronous-within-each-thread facility. There is no support for asynchronous operation. If you require asynchronous operation, you must write directly to the nCore API.

For more information about the way the CHIL interface works with the nShield APIs, see Figure 3.

For more information about using the available libraries, see the **`Include Paths and Linking`** section in the *nCore API Documentation* provided in HTML form on the Security World Software installation media.

4.1 Structures the application must provide

Your application must define the structures described in this section. They are opaque to the CHIL plug-in. Your application may define them as it sees fit.

These structures are required if your application is multi-threaded:

```
typedef struct HWCryptoHook_MutexValue HWCryptoHook_Mutex;
typedef struct HWCryptoHook_CondVarValue HWCryptoHook_CondVar;
```

This structure is required if your application supports keys or cards protected by pass phrases:

```
typedef struct HWCryptoHook_PassphraseContextValue HWCryptoHook_PassphraseContext;
```

This structure is required if your application passes non-**`NULL`** values of context parameter to **`hwcrhk`** functions for the library to pass on to pass phrase or card change callbacks:

```
typedef struct HWCryptoHook_CallerContextValue HWCryptoHook_CallerContext;
```

The header files supplied by nCipher provide the above declarations for these structures. If you want to use your own declarations, define the following before including **`hwcryptohook.h`** to prevent these declarations:

```
#define HWCRYPTOHOOK_DECLARE_APPTYPES 0
```

ℹ If you define your own structures, the pointers to these structures must be ordinary pointers to **`structs`** or **`unions`**, otherwise the resulting combined program have type inconsistencies.

4.2 Structures provided by hwcrhk

The following structures are defined by the CHIL plug-in and are opaque to the application:

```
typedef struct HWCryptoHook_Context *HWCryptoHook_ContextHandle;
typedef struct HWCryptoHook_RSAKey *HWCryptoHook_RSAKeyHandle;
typedef struct HWCryptoHook_DHKey *HWCryptoHook_DHKeyHandle;
typedef struct HWCryptoHook_DSAKey *HWCryptoHook_DSAKeyHandle;
```

The CHIL plug-in returns pointers to these structures. The caller simply manipulates the pointers.

4.3 Multi-precision integers

RSA operations require large integers consisting of hundreds of bytes.

CHIL expects multi-precision integers to be stored as an array of limbs, each of which consists of a number of bytes. For example, each limb might be a 4-byte word in native byte order.

When you initialize the library, you set the limb size, the order of limbs within an integer, and the order of the bytes within a limb. You can choose whatever settings are most suitable for your application, but all the multi-precision integers within an application must use the same settings.

Zero limbs at the Most Significant end are not permitted. The multi-precision value 0 is represented with no limbs (`size==0`).

CHIL uses the following structure to hold multi-precision integers:

```
typedef struct HWCryptoHook_MPIStruct {
        unsigned char *buf;
        size_t size;
} HWCryptoHook_MPI;
```

In this structure:

- `*buf`

  This is a pointer to the buffer holding the multi-precision integer or available for the library to return a multi-precision integer. The library does not update this pointer.

- `size`

  The size of the buffer in bytes. When the library returns a multi-precision integer, it is set to the actual size of the multi-precision integer. The `size` can be `0` but must be a multiple of the limb size, which is set in the `HWCryptoHook_InitInfo`.

4.4 Handling errors

When a `HWCryptoHook` function fails, it returns an error value. This value is:

- `0` for pointer-valued functions
- a negative number for integer-valued functions.

`HWCRYPTOHOOK_ERROR_FAILED` means that the failure is permanent and definite and that there should be no attempt to fall back to software. For applications that support just the acceleration functions, the "key material" can be an encoded key identifier; doing the operation in software would give incorrect answers.

`HWCRYPTOHOOK_ERROR_FALLBACK` means that doing the computation in software would seem reasonable. If an application pays attention to this value and is able to fall back, it should also set the `Fallback` init flags.

`HWCRYPTOHOOK_ERROR_MPISIZE` means that the output multi-precision integer buffer was full. The `size` has been set to the desired size.

Additionally, if you passed an `ErrMsgBuf` to the function, it outputs an error message there.

```
typedef struct {
        char *buf;
        size_t size;
} HWCryptoHook_ErrMsgBuf;
```

In this structure:

- **`*buf`**

  This is a pointer to the buffer. If you pass a NULL pointer, you must set **`size`** to 0, and nothing is recorded.

- **`size`**

  The value **`size`** is the size of the buffer. This value is not modified when an error is recorded.

When the buffer is filled, it is always null-terminated.

4.5 HWCryptoHook_Init

This function initializes the Cryptographic Hardware Interface Library (CHIL).

`HWCryptoHook_Init` takes a **`HWCryptoHook_InitInfo`** structure that includes settings for multi-precision integers and a pointer to the functions used for mutexes, condition variables, and the callback functions that provide the user interface.

All the callback functions must return 0 on success, or a nonzero integer (whose value is visible in the error message put in the buffer passed to the call). If a callback is not available, pass a null function pointer. The callbacks do not call down again into the CHIL plug-in.

A single operation might cause several calls to **`getpassphrase`** and **`requestphystoken`**. It is not necessary for **`getpassphrase`** or **`getphystoken`** to check that the pass phrase has been entered correctly or that the correct token has been inserted; the CHIL plug-in makes these checks. If the pass phrase has not been entered correctly, then the CHIL plug-in is responsible for calling these routines again, as appropriate, until the correct token(s) and pass phrase(s) are supplied as required or until any retry limits implemented by the CHIL plug-in are reached. For either callback, the application must allow the user to say “No” or “Cancel” to indicate that they neither know the pass phrase nor have the appropriate token. This situation should cause the callback to a return nonzero, indicating an error:

```
typedef
HWCryptoHook_ContextHandle HWCryptoHook_Init_t(const
  HWCryptoHook_InitInfo *initinfo,
                size_t initinfosize,
                const
  HWCryptoHook_ErrMsgBuf *errors,
  HWCryptoHook_CallerContext *cactx);
extern HWCryptoHook_Init_t HWCryptoHook_Init;
```

This function writes a message that includes the name and version number of the plug-in to **`msgbuf`**. In this function:

- **`initinfosize`**

  This is the size of the **`HWCryptoHook_InitInfo`** structure.

- **`initinfo`**

  This is a pointer to a **`HWCryptoHook_InitInfo`** structure:

```
typedef struct {
unsigned long flags;
FILE *logstream;
size_t limbsize;
int mslimbfirst;
int msbytefirst;
int maxmutexes;
int maxsimultaneous;
size_t mutexsize;
int (*mutex_init)(HWCryptoHook_Mutex*, HWCryptoHook_CallerContext *cactx);
int (*mutex_acquire)(HWCryptoHook_Mutex*);
void (*mutex_release)(HWCryptoHook_Mutex*);
void (*mutex_destroy)(HWCryptoHook_Mutex*);
size_t condvarsize;
int (*condvar_init)(HWCryptoHook_CondVar*, HWCryptoHook_CallerContext *cactx);
int (*condvar_wait)(HWCryptoHook_CondVar*, HWCryptoHook_Mutex*);
void (*condvar_signal)(HWCryptoHook_CondVar*);
void (*condvar_broadcast)(HWCryptoHook_CondVar*);
void (*condvar_destroy)(HWCryptoHook_CondVar*);
int (*getpassphrase)(const char *prompt_info,
      int *len_io,
      char *buf,
      HWCryptoHook_PassphraseContext *ppctx,
      HWCryptoHook_CallerContext *cactx);
int (*getphystoken)(const char *prompt_info,
      const char *wrong_info,
      HWCryptoHook_PassphraseContext *ppctx,
      HWCryptoHook_CallerContext *cactx);
void (*logmessage)(void *logstream, const char *message);
void *(*malloc_hook)(size_t, HWCryptoHook_CallerContext *cactx);
void *(*realloc_hook)(void*, size_t, HWCryptoHook_CallerContext *cactx);
void (*free_hook)(void*, HWCryptoHook_CallerContext *cactx);
} HWCryptoHook_InitInfo;
```

In this structure:

- **unsigned long flags**

  The following flags are defined:

  - **#define HWCryptoHook_InitFlags_FallbackModExp 0x02UL**

    This flag enables requests for fallback to software in case of problems with the hardware support. It indicates to the cryptographic provider that the application is prepared to fall back to software operation if the `ModExp*` or `RSAImmed*` functions return **HWCRYPTOHOOK_ERROR_FALLBACK**. If this flag is not set, the function never returns **HWCRYPTOHOOK_ERROR_FALLBACK**. The flag also causes the cryptographic provider to avoid repeated attempts to contact dead hardware within a short interval, if appropriate.

  - **#define HWCryptoHook_InitFlags_FallbackRSAImmed 0x04UL**

    This flag enables requests for fallback to software in case of problems with the hardware support. It indicates to the cryptographic provider that the application is prepared to fall back to software operation if the `ModExp*` or `RSAImmed*` functions return **HWCRYPTOHOOK_ERROR_FALLBACK**. If this flag is not set, the function never returns **HWCRYPTOHOOK_ERROR_FALLBACK**. The flag also causes the cryptographic provider to avoid repeated attempts to contact dead hardware within a short interval, if appropriate.

  - **#define HWCryptoHook_InitFlags_SimpleForkCheck 0x0010UL**

If this flag is not set, the library is allowed to assume that the application does not fork and to call the library in the child process (or processes). When this flag is set, such functionality is allowed. However, after a fork, neither parent nor a child process can unload any loaded keys or call **`HWCryptoHook_Finish`**. Instead, they should call exit (or die with a signal) without calling **`HWCryptoHook_Finish`**. After all the children have died, the parent may unload keys or call **`HWCryptoHook_Finish`**.

This flag only has the desired effect on Unix platforms.

- **`*logstream`**

  A log message is generated at least every time something goes wrong, and an **`ErrMsgBuf`** is filled in (or would be filled in if one were provided). Other diagnostic information can also be written to the log message, including more detailed reasons for errors that are reported in an **`ErrMsgBuf`**. When a log message is generated, a message is sent to the logstream if the logstream is nonzero.

  The CHIL plug-in may also provide facilities to specify that copies of log messages be sent elsewhere and make adjustments to the verbosity of the log messages.

  Log messages consist of whole lines. Each line is prefixed by a descriptive string containing the date, time, and identity of the CHIL plug-in. This descriptive string ends at the first occurrence of the string ": " (that is, a colon followed by a space) in the message. Errors on the logstream are not reported anywhere.

- **`limbsize`**

  This is the size in bytes of limbs within multi-precision integers. It must be a power of 2.

- **`mslimbfirst`**

  This is the order of limbs within multi-precision integers:

  - 1 (most significant limb first)
  - 0 (least significant limb first).

- **`msbytefirst`**

  This is the order of bytes within a limb, which is independent of the order of the limbs themselves:

  - 1 (most significant byte first)
  - 0 (least significant byte first)
  - -1 (native order for the platform).

- **`*maxmutexes`**

  This is a small limit on the number of simultaneous mutexes that are requested by the library. If there is no small limit, set it to **`0`**.

  If the CHIL plug-in cannot create the advertised number of mutexes, the calls to its functions may fail. If a low number of mutexes is advertised, the plug-in does the best it can. Making larger numbers of mutexes available may improve performance and parallelism by reducing contention over critical sections.

  Unavailability of any mutexes, implying single-threaded operation, should be indicated by the setting the mutex pointers to **`NULL`**.

- **`maxsimultaneous`**

  This sets **`maxsimultaneous`** to the maximum number of simultaneous calls to the modulo exponentiation functions that your application makes. If you do not know what this number is, set this value to **`0`** in order to make the library use a default value.

- **`mutexsize`**

  The semantics of acquiring and releasing mutexes, and broadcasting and waiting on condition variables, are expected to be those from POSIX threads (pthreads). The mutexes may be (in the terminology of pthread) fast mutexes, recursive mutexes, or nonrecursive mutexes.

  The **`mutex_release`**, **`condvar_signal`**, **`condvar_broadcast`**, and **`condvar_destroy`** functions must always succeed when given a valid argument. If they are given an invalid argument, then the program (that is, the CHIL plug-in and the application) has an internal error, and they should abort the program.

  In single-threaded programs, set all mutex and condition variable entries to **`0`**.

- **`condvarsize`**

  For greater efficiency, the plug-in may use condition variables internally for synchronization. In this case, **`maxsimultaneous`** is ignored, but the mutex functions must be available.

- **`int (*getpassphrase)(const char *prompt_info`**

  This is a pointer to the callback function used to prompt the user for a pass phrase. If this pointer is set to **`NULL`**, the program can not use Operator Card Sets protected by pass phrases. Pass phrases and the **`prompt_info`**, if they contain high-bit-set characters, are UTF-8. The **`prompt_info`** can be a null pointer if no prompt information is available (it cannot be an empty string). It cannot contain text like “enter pass phrase”; instead its text should be of a form like “Operator Card for John Smith” or “SmartCard in Module#1, Slot#1”.

- **`int (*getphystoken)(const char *prompt_info`**

  This flag requests that the human user physically insert a different smart card. The plug-in checks to see whether the currently inserted token or tokens are appropriate. If they are, the plug-in does make this call. If you pass a **`NULL`** pointer for **`requestphystoken`**, the program does not support loading keys if either the key requires authorization by several cards or the card protecting the key is not present when the key is loaded.

  `* prompt_info` is as for **`getpassphrase`** (see *HWCryptoHook_Init* on page 57). **`wrong_info`** is a description of the currently inserted token(s) so that the user is told what something is. **`wrong_info`** is a description of the currently inserted token(s) so that the user is told what something is. **`wrong_info`**, like **`prompt_info`**, can be null, but cannot be an empty string. Its contents are syntactically similar to that of **`prompt_info`**.

- **`void (*logmessage)(void *logstream, const char *message);`**

  This is the size of the **`HWCryptoHook_InitInfo`** structure.

- **`void *(*malloc_hook)(size_t, HWCryptoHook_CallerContext *cactx);,`**
- **`void *(*realloc_hook)(void*, size_t, HWCryptoHook_CallerContext *cactx);,`**
- **`void (*free_hook)(void*, HWCryptoHook_CallerContext *cactx);`**

  Pass **`0`** in order to use the standard C library **`malloc/realloc/free`**. If callbacks are supplied, they must have standard ANSI C89 semantics.

4.6 HWCryptoHook_RandomBytes

This command returns a block of bytes filled with random data generated by the module’s on-board hardware random number generator.

```
typedef
int HWCryptoHook_RandomBytes_t(HWCryptoHook_ContextHandle hwctx,
    unsigned char *buf,
    size_t len,
    const HWCryptoHook_ErrMsgBuf *errors);
extern HWCryptoHook_RandomBytes_t HWCryptoHook_RandomBytes;
```

In this command:

- **`hwctx`**

  This is returned by **`HWCryptoHook_Init`**.
- **`*buf`**

  This is a pointer to a buffer to hold the returned bytes.
- **`len`**

  This is the size of the buffer in bytes.

4.7 HWCryptoHook_ModExp & HWCryptoHook_RSAImmedPub

These commands perform a modulo exponentiation on multi-precision integers supplied with the command.

```
typedef
int HWCryptoHook_ModExp_t(HWCryptoHook_ContextHandle hwctx,
        HWCryptoHook_MPI a,
        HWCryptoHook_MPI p,
        HWCryptoHook_MPI n,
        HWCryptoHook_MPI *r,
const HWCryptoHook_ErrMsgBuf *errors); extern HWCryptoHook_ModExp_t HWCryptoHook_ModExp;
```

```
typedef
int HWCryptoHook_RSAImmedPub_t(HWCryptoHook_ContextHandle hwctx,
        HWCryptoHook_MPI m,
        HWCryptoHook_MPI e,
        HWCryptoHook_MPI n,
        HWCryptoHook_MPI *r,
const HWCryptoHook_ErrMsgBuf *errors); extern HWCryptoHook_RSAImmedPub_t HWCryptoHook_
RSAImmedPub;
```

In this command:

- **`HWCryptoHook_MPI a`**

  A base.

- **HWCryptoHook_MPI p**

  P power.

- **HWCryptoHook_MPI n**

  N modulus.

- **HWCryptoHook_MPI *r**

  = A^P MOD$_N$.

- **HWCryptoHook_MPI m**

  Message.

- **HWCryptoHook_MPI e**

  Exponent.

- **HWCryptoHook_MPI n**

  Key modulus.

- **HWCryptoHook_MPI *r**

  Result.

4.8 HWCryptoHook_ModExpCRT and HWCryptoHook_RSAImmedPriv

These commands perform modulo exponentiation using the Chinese Remainder Theorem on multi-precision integers supplied with the command. Use **HWCryptoHook_RSALoadKey** and **HWCryptoHook_RSA** to perform these operations on stored keys.

```
typedef
int HWCryptoHook_ModExpCRT_t(HWCryptoHook_ContextHandle hwctx,
        HWCryptoHook_MPI a,
        HWCryptoHook_MPI p,
        HWCryptoHook_MPI q,
        HWCryptoHook_MPI dmp1,
        HWCryptoHook_MPI dmq1,
        HWCryptoHook_MPI iqmp,
        HWCryptoHook_MPI *r,
        const HWCryptoHook_ErrMsgBuf *errors);
extern HWCryptoHook_ModExpCRT_t HWCryptoHook_ModExpCRT;
```

```
typedef
int HWCryptoHook_RSAImmedPriv_t(HWCryptoHook_ContextHandle hwctx,
        HWCryptoHook_MPI m,
        HWCryptoHook_MPI p,
        HWCryptoHook_MPI q,
        HWCryptoHook_MPI dmp1,
        HWCryptoHook_MPI dmq1,
        HWCryptoHook_MPI iqmp,
        HWCryptoHook_MPI *r,
        const HWCryptoHook_ErrMsgBuf *errors);
extern HWCryptoHook_RSAImmedPriv_t HWCryptoHook_RSAImmedPriv;
```

In these commands:

- **`HWCryptoHook_MPI a`**

  A base

- **`HWCryptoHook_MPI p`**

  - **`HWCryptoHook_ModExpCRT`**

    P modulus larger factor.

  - **`HWCryptoHook_RSAImmedPriv`**

    First factor.

- **`HWCryptoHook_MPI q`**

  - **`HWCryptoHook_ModExpCRT`**

    Q modulus smaller factor.

  - **`HWCryptoHook_RSAImmedPriv`**

    Second factor.

- **`HWCryptoHook_MPI dmp1`**

  D MOD_{P-1}.

- **`HWCryptoHook_MPI dmq1`**

  D MOD_{Q-1}.

- **`HWCryptoHook_MPI iqmp`**

  Q^{-1} MOD_{P}.

- **`HWCryptoHook_MPI *r`**

  Result.

- **`HWCryptoHook_MPI m`**

  Ciphertext.

4.9 HWCryptoHook_RSALoadKey

This function loads a private key from a key store. You can then use **`HWCryptoHook_RSA`** to perform decryptions or signatures with this key. Use **`HWCryptoHook_RSAUnloadKey`** to unload the key when you have finished using it.

To perform encryptions or verifications using a public key, use **`HWCryptoHook_RSAGetPublicKey`** and then **`HWCryptoHook_RSAImmedPub.`**

The function may issue a callback to **`getphystoken`** or **`getpassphrase`**.

```
typedef
int HWCryptoHook_RSALoadKey_t(HWCryptoHook_ContextHandle hwctx,
        const char *key_ident,
        HWCryptoHook_RSAKeyHandle *keyhandle_r,
        const HWCryptoHook_ErrMsgBuf *errors,
        HWCryptoHook_PassphraseContext *ppctx);
extern HWCryptoHook_RSALoadKey_t HWCryptoHook_RSALoadKey
```

In this function:

- ***key_ident**

  This is a null-terminated string configured by the user through the application's usual configuration mechanisms. It is provided to the user by the cryptographic provider's key-management system. The user must be able to enter at least any string of between 1 and 1023 characters inclusive that consists of printable 7-bit ASCII characters. The provider avoids using any characters except alphanumeric characters and the punctuation characters _ - + . / @ ~ (the user is expected to be able to enter these without quoting). The string can be case sensitive. The application can allow the user to enter other null-terminated strings, and the provider must cope (returning an error if the string is not valid).

- ***keyhandle_r**

  If the key does not exist, **keyhandle_r** is set to **0** instead of to a key handle. This is not an error.

4.10 HWCryptoHook_RSA

This function performs an RSA decryption using a previously loaded private key.

```
typedef
int HWCryptoHook_RSA_t(HWCryptoHook_MPI m,
        HWCryptoHook_RSAKeyHandle k,
        HWCryptoHook_MPI *r,
        const HWCryptoHook_ErrMsgBuf *errors);
extern HWCryptoHook_RSA_t HWCryptoHook_RSA;
```

In this function:

- **HWCryptoHook_MPI m**

  This is a message to decrypt or sign. The message must have been padded according to the appropriate specification. The **HWCryptoHook_RSA** function only completes **M**^{d} **mod N**.

- **HWCryptoHook_RSAKeyHandle k**

  This is a key handle returned by **HWCryptoHook_RSALoadKey.**

- **HWCryptoHook_MPI *r**

  This is the plain text returned.

4.11 HWCryptoHook_RSAUnloadKey

This function unloads an RSA key that you have previously loaded.

```
typedef
int HWCryptoHook_RSAUnloadKey_t(HWCryptoHook_RSAKeyHandle k,
        const HWCryptoHook_ErrMsgBuf *errors);
extern HWCryptoHook_RSAUnloadKey_t HWCryptoHook
```

In this function **HWCryptoHook_RSAKeyHandle k** is the key handle returned by **HWCryptoHook_RSALoadKey**. It fails only when there are locking problems or other serious internal problems.

4.12 HWCryptoHook_RSAGetPublicKey

This function returns the public half of a key pair identified by a key handle.

Although this function is provided for acquiring the public key value, it is not the purpose of this API to deal fully with the handling of the public key.

The CHIL plug-in does not store certificates. It is expected that the CHIL supplier's key-generation program provides general facilities for producing X.509 self-certificates and certificate requests in PEM format, which the application should be able to import. If this certificate handling is not appropriate, the application should instruct the user not to use the provider's tools to generate certificate requests. Instead the application should use **`HWCryptoHook_RSAGetPublicKey`** and generate and store appropriate certificates and requests itself.

```
typedef
int HWCryptoHook_RSAGetPublicKey_t(HWCryptoHook_RSAKeyHandle k,
        HWCryptoHook_MPI *n,
        HWCryptoHook_MPI *e,
        const HWCryptoHook_ErrMsgBuf *errors);
extern HWCryptoHook_RSAGetPublicKey_t HWCryptoHook_RSAGetPublicKey;
```

In this function:

- **`HWCryptoHook_RSAKeyHandle k`**

  This is the key handle returned by **`HWCryptoHook_RSALoadKey`**.
- **`HWCryptoHook_MPI *n`**

  This is the public key modulus.
- **`HWCryptoHook_MPI *e`**

  This is the public key exponent.

4.13 HWCryptoHook_DHLoadKey

This function loads a private key from a key store. You can then use **`HWCryptoHook_DH`** to perform a key exchange with this key. Use **`HWCryptoHook_DHUnloadKey`** to unload the key when you have finished using it.

```
typedef
int HWCryptoHook_DHLoadKey_t(HWCryptoHook_ContextHandle hwctx,
        const char *key_ident,
        HWCryptoHook_DHKeyHandle *keyhandle_r,
        const HWCryptoHook_ErrMsgBuf *errors,
        HWCryptoHook_PassphraseContext *ppctx);
extern HWCryptoHook_DHLoadKey_t HWCryptoHook_DHLoadKey;
```

In this function:

- **`*key_ident`**

  This is a null-terminated string configured by the user through the application's usual configuration mechanisms. It is provided to the user by the cryptographic provider's key-management system. The user must be able to enter at least any string of between 1 and 1023 characters inclusive that consists of printable 7-bit ASCII characters. The provider avoids using any characters except alphanumeric characters and the punctuation characters _ `- + . / @` ~ (the user is expected to be able to enter these without quoting). The string can be case sensitive. The application can allow the user to enter other null-terminated strings, and the provider must cope (returning an error if the string is not valid).

- **`*keyhandle_r`**

  If the key does not exist, **`keyhandle_r`** is set to **`0`** instead of to a key handle. This is not an error.

4.14 HWCryptoHook_DH

This function performs a Diffie-Hellman key exchange using a previously loaded private key.

```
typedef
int HWCryptoHook_DH_t(HWCryptoHook_MPI gx,
HWCryptoHook_DHKeyHandle k,
HWCryptoHook_MPI *r,
const HWCryptoHook_ErrMsgBuf *errors);
extern HWCryptoHook_DH_t HWCryptoHook_DH;
```

In this function:

- **`gx`**

  `gx` is the public key value of the other party.

- **`k`**

- **`k`** is a key handle returned by HWCryptoHook_DHLoadKey.

  `r`

- **`r`** is the shared secret returned.

  The public value **`gx`** and the private key **`k`** are assumed to share the same discrete log group parameters.

4.15 HWCryptoHook_DHUnloadKey

This function unloads a Diffie-Hellman key that you have previously loaded.

```
typedef
int HWCryptoHook_DHUnloadKey_t(HWCryptoHook_DHKeyHandle k,
const HWCryptoHook_ErrMsgBuf *errors);
extern HWCryptoHook_DHUnloadKey_t HWCryptoHook_DHUnloadKey;
```

In this function **k** is the key handle returned by **HWCryptoHook_DHLoadKey**. It fails only when there are locking problems or other serious internal problems.

4.16 HWCryptoHook_DHGetPublicKey

This function returns the public half of a key pair identified by a key handle.

Although this function is provided for acquiring the public key value, it is not the purpose of this API to deal fully with the handling of the public key.

The CHIL plug-in does not store certificates. It is expected that the cryptographic supplier's key-generation program provides general facilities for producing X.509 self-certificates and certificate requests in PEM format, which the application should be able to import. If this certificate handling is not appropriate, the application should instruct the user not to use the provider's tools to generate certificate requests. Instead the application should use **HWCryptoHook_DHGetPublicKey** and generate and store appropriate certificates and requests itself.

```
typedef
int HWCryptoHook_DHGetPublicKey_t(HWCryptoHook_DHKeyHandle k,
HWCryptoHook_MPI *p,
HWCryptoHook_MPI *g,
HWCryptoHook_MPI *gx,
const HWCryptoHook_ErrMsgBuf *errors);
extern HWCryptoHook_DHGetPublicKey_t HWCryptoHook_DHGetPublicKey;
```

In this function:

- **p**

  p is the prime from the discrete log group.
- **g**

  g is the generator from the discrete log group.
- **gx**

  gx is the public key value.

4.17 HWCryptoHook_DSALoadKey

This function loads a private key from a key store. You can then use **HWCryptoHook_DSA** to perform signing operation with this private key. Use **HWCryptoHook_DSAUnloadKey** to unload the key when you have finished with it.

```
typedef
int HWCryptoHook_DSALoadKey_t(HWCryptoHook_ContextHandle hwctx,
const char *key_ident,
HWCryptoHook_DSAKeyHandle *keyhandle_r,
const HWCryptoHook_ErrMsgBuf *errors,
HWCryptoHook_PassphraseContext *ppctx);
extern HWCryptoHook_DSALoadKey_t HWCryptoHook_DSALoadKey;
```

In this function:

- **`*key_ident`**

  This is a null-terminated string configured by the user through the application's usual configuration mechanisms. It is provided to the user by the cryptographic provider's key-management system. The user must be able to enter at least any string of between 1 and 1023 characters inclusive that consists of printable 7-bit ASCII characters. The provider avoids using any characters except alphanumeric characters and the punctuation characters _ `- + . / @` and ~(the user is expected to be able to enter these without quoting). The string can be case sensitive. The application can allow the user to enter other null-terminated strings, and the provider must cope (returning an error if the string is not valid).
- **`*keyhandle_r`**

  If the key does not exist, **`keyhandle_r`** is set to **`0`** instead of to a key handle. This is not an error.

4.18 HWCryptoHook_DSA

This function performs a DSA signing operation with a previously loaded private key.

```
typedef
int HWCryptoHook_DSA_t(const unsigned char *h,
HWCryptoHook_DSAKeyHandle k,
HWCryptoHook_MPI *r,
HWCryptoHook_MPI *s,
const HWCryptoHook_ErrMsgBuf *errors;
extern HWCryptoHook_DSA_t HWCryptoHook_DSA;
```

In this function:

- **`*h`**

  `h` is expected to be a 20-byte SHA-1 hash.
- **`k`**

  `k` is a key handle returned by HWCryptoHook_DSALoadKey.
- **`*r`**

  `r` is the **`r`**-value of the signature returned.
- **`*s`**

  `s` is the **`s`**-value of the signature returned.

4.19 HWCryptoHook_DSAUnloadKey

This function unloads a DSA key that you have previously loaded.

```
typedef
int HWCryptoHook_DSAUnloadKey_t(HWCryptoHook_DSAKeyHandle k,            See 1 below
const HWCryptoHook_ErrMsgBuf *errors);
extern HWCryptoHook_DSAUnloadKey_t HWCryptoHook_DSAUnloadKey;
```

In this function **k** is the key handle returned by **HWCryptoHook_DSALoadKey**. It fails only when there are locking problems or other serious internal problems.

4.20 HWCryptoHook_DSAGetPublicKey

This function returns the public half of a key pair identified by a key handle.

Although this function is provided for acquiring the public key value, it is not the purpose of this API to deal fully with the handling of the public key.

The CHIL plug-in does not store certificates. It is expected that the cryptographic supplier's key-generation program provides general facilities for producing X.509 self-certificates and certificate requests in PEM format, which the application should be able to import. If this certificate handling is not appropriate, the application should instruct the user not to use the provider's tools to generate certificate requests. Instead, applications should use **HWCryptoHook_DSAGetPublicKey** and generate and store appropriate certificates and requests itself.

```
typedef
int HWCryptoHook_DSAGetPublicKey_t(HWCryptoHook_DSAKeyHandle k,
HWCryptoHook_MPI *p,
HWCryptoHook_MPI *q,
HWCryptoHook_MPI *g,
HWCryptoHook_MPI *y,
const HWCryptoHook_ErrMsgBuf *errors);
extern HWCryptoHook_DSAGetPublicKey_t HWCryptoHook_DSAGetPublicKey;
```

In this function:

- ***p**

  p is the prime from the discrete log group.

- ***q**

  q is the **q** value from the discrete log group (A 160-bit prime factor of **p-1**).

- ***g**

  g is the generator from the discrete log group.

- ***y**

  y is the public key value.

4.21 HWCryptoHook_Finish

This function closes the CHIL session. You must not have any calls going or keys loaded when you call this function.

```
typedef
void HWCryptoHook_Finish_t(HWCryptoHook_ContextHandle hwctx);
extern HWCryptoHook_Finish_t HWCryptoHook_Finish;
```

4.22 CHIL error logging

Error message logging is implemented in CHIL using the **`logmessage`** callback defined in **`hwcryptohook.h`**:

```
  void (*logmessage)(void *logstream, const char *message);
```

When a log message is generated, this callback is called. It should write a message to the relevant logging arrangements. A log message is generated at least every time something goes wrong and an **`ErrMsgBuf`** is filled in (or would be if one was provided). Other diagnostic information may be written there too, including more detailed reasons for errors which are reported in an **`ErrMsgBuf`**.

The message string passed is null-terminated and can be of arbitrary length. It is not prefixed by the time and date, nor by the name of the library that is generating it; if this is required, the **`logmessage`** callback must do it. The message does not have a trailing newline (though it can contain internal newlines).

If a null pointer is passed for **`logmessage`** a default function is used. The default function treats **`logstream`** as a **`FILE*`** which has been converted to a **`void*`**. If **`logstream`** is 0 (zero) it does nothing. Otherwise it adds the date and time and library name to the beginning of the message and writes it to **`logstream`**. Each line is prefixed by a descriptive string containing the date, time and identity of the cryptographic plug-in. Errors on **`logstream`** are not reported anywhere, and the default function doesn’t flush the stream, so the application must set the buffering how it wants it.

The cryptographic plug-in may also provide a facility to have copies of log messages sent elsewhere, and/or for adjusting the verbosity of the log messages; any such facilities must be configured by some means external to the CHIL.

The CHIL API permits the plug-in to return a single-line error string for each call. This error string sometimes contains a list of errors, in a form like this:

```
Failed to load key (codes: m1MU m2b0BL28 m2BN)
```

Each code consists of a sequence of alphanumeric characters, comprised of:

- optional prefixes, identifying where the error occurred
- a 2-character error code
- an optional suffix.

These codes are an important diagnostic tool, and are useful for debugging.

The following table lists the prefixes, suffixes and their meanings:

Code	Meaning
Prefixes	

Code	Meaning
m	On module # (for module 1, m=1).
b	Blob # (usually there is only one blob, which is numbered b0).
s	Slot # (usually s0).
i	Share index # (usually i1).
Suffixes	
#	Trailing digits are a status code value.
*	A numerical value (see details of message).
&	Integer from **`getphystoken`**/**`getpassphrase`** upcall.

The following table lists the error codes and the corresponding long messages which appear in the log file(s).

Error code	Long message
MQ	Module in unknown state.
MM	Module in maintenance mode.
MU	Module in uninitialized mode.
MF	Module has failed.
MP	Module in Pre-Init mode.
MS*	Module in strange state (* is an NFKM library state code).
BE#	Blob Examine failed.
BR	Blob requires recovery key.
BL#	Blob Load failed.
BN	Blob(s) not found or unsuitable (after other B… codes).
CU	Card set protecting blob is unknown.
CI#	Card info unavailable.
MNA	Module no longer available.
CB#	Card set begin loading failed.
SE	Slot empty.
SC*	Slot does not contain operator card (* is NFKM card code).
SD	Slot contains different operator card.

Error code	Long message
SA	Slot contains card/share already loaded.
CP	Card has a pass phrase, cannot load.
PR&	Pass phrase read failed.
PH#	Pass phrase hash failed.
CRU#	Card read failed with unexpected error.
CR#	Card read failed.
PI	Pass phrase incorrect.
CA	Card(s) inserted are not (yet) appropriate.
CN&	Card(s) needed but not acquired.
CF#	Card loading finish failed.

4.22.1 Example

```
Failed to load key (codes: m1MU m2b0BL28 m2BN)
```

The example error message above indicates that:

- CHIL tried to load the key on module #1, but it was in uninitialized mode
- CHIL then tried to load the key on module 2. Trying the first blob for the key (usually a key has only one blob) on module #2, it got error Status 28 from **LoadBlob** (that is **UnknownKM**). This indicates that the module is probably not programmed into the correct Security World.)
- the third code is just a confirmation that no suitable blobs were found for module 2.

Because the key was not loaded on any module, the operation failed.

5 Microsoft CAPI CSP

We provide a Cryptographic Service Provider (CSP) that implements the Crypto API (CAPI) supported in Windows 2008 and later.

The rest of this chapter details the features and implementation details of the CAPI. Except where this chapter specifies otherwise, the Security World Software implementation conforms to the Microsoft CSP interface. For more information, see the Microsoft CSP documentation.

5.1 Crypto API CSP

The following provider types are supported:

- **`PROV_RSA_FULL`** (nShield Enhanced Cryptographic Provider)
- **`PROV_RSA_AES`** (nShield Enhanced RSA and AES Cryptographic Provider)
- **`PROV_RSA_SCHANNEL`** (nShield Enhanced SChannel Cryptographic Provider)
- **`PROV_DSS`** (nShield DSS Signature Cryptographic Provider)
- **`PROV_DSS_DH`** (nShield Enhanced DSS and Diffie-Hellman Cryptographic Provider)
- **`PROV_DH_SCHANNEL`** (nShield Enhanced DSS and Diffie-Hellman SChannel Cryptographic Provider)

We also provide a modulo exponentiation offload DLL that enables the Microsoft CSP to take advantage of the computational power of an nShield module without added security benefits. This is useful for interoperation with applications that do not allow the user to choose the CSP.

ℹ Unlike the Microsoft CSPs, the nShield CSPs do not support the exporting of private keys.

You should not need to make any adjustments to your code in order to use the nShield CSPs. However, the nShield module is an asynchronous device capable of performing several operations at once. In order to achieve maximum performance from the module, structure your application in a multithreaded manner so that it can make several simultaneous requests to the CSP.

Figure 4. Microsoft CryptoAPI architecture

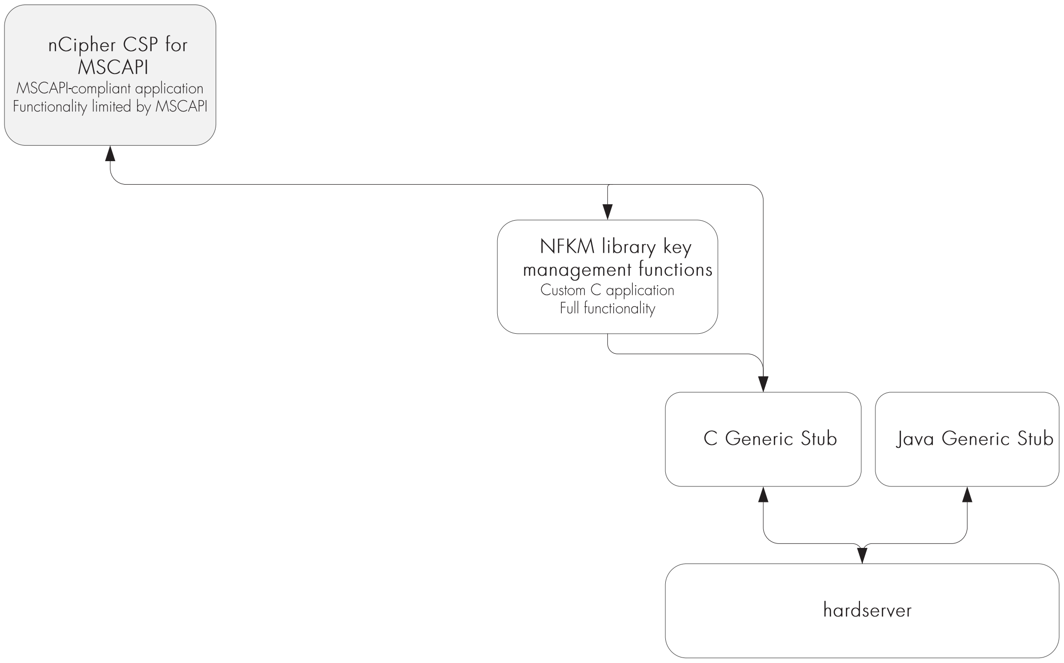


Figure 4 shows the way that the Microsoft CryptoAPI interface works with the nShield APIs.

5.2 Supported algorithms

The nShield CSPs support a similar range of algorithms to the Microsoft CSP.

5.2.1 Symmetric algorithms

- `CALG_DES`
- `CALG_3DES_112` (double-DES)
- `CALG_3DES`
- `CALG_RC4`
- `CALG_AES_128`
- `CALG_AES_192`
- `CALG_AES_256`

5.2.2 Asymmetric algorithms

- `CALC_RSA_SIGN` (only Enhanced RSA and AES Cryptographic Provider)
- `CALC_RSA_KEYX` (only Enhanced RSA and AES Cryptographic Provider)
- `CALC_DSA_SIGN` (only Enhanced DSS and Diffie-Hellman Cryptographic Provider and DSS Signature Cryptographic Provider)
- `CALC_DSS_SIGN` (only Enhanced DSS and Diffie-Hellman Cryptographic Provider)
- `CALC_DH_KEYX` (only Enhanced DSS and Diffie-Hellman Cryptographic Provider)

- **`CALC_DH_SF`** (only Enhanced DSS and Diffie-Hellman Cryptographic Provider)
- **`CALC_DH_EPHEM`** (only Enhanced DSS and Diffie-Hellman Cryptographic Provider)

5.2.3 Hash algorithms

- **`CALG_SHA1`**
- **`CALG_SHA256`**
- **`CALG_SHA384`**
- **`CALG_SHA512`**
- **`CALG_SSL3_SHAMD5`**
- **`CALG_MD5`**
- **`CALG_MAC`**
- **`CALG_HMAC`**

In addition, the Enhanced SChannel Cryptographic Provider and the Enhanced DSS and Diffie-Hellman SChannel Cryptographic Provider support all the internal algorithm types necessary for SSL3 and TLS1 support.

The nShield CSPs do not support SSL2.

5.3 Key generation and storage

The nShield CSP generates public/private key pairs (RSA, DSA, and Diffie-Hellman keys) in the module. The keys are stored in the Security World as protected by key blobs. (For details of the Security World, see the User Guide). Natively generated keys have **`mscapi`** as the **`appname`** and the hash of the key as the **`ident`**.

As in the Microsoft CSP, up to two keys are allowed for each container. Containers themselves are stored as opaque data in the Security World. Containers contain no key information but serve to associate NFKM keys with CSP containers, as well as storing other miscellaneous information. They have **`mscapi`** as the **`appname`** and **`container-`***containerID* as the **`ident`**, where *containerID* is calculated from a combination of the CSP name, the user's unique SID and the container name.

The default permissions on new containers created by the nShield CSP have changed in order to solve a problem with IIS version 6: in this version of IIS it was possible to create containers with an empty ACL, such that they were completely inaccessible.

The previous default container permissions came from the inherited permissions on the **`NFAST_KMLOCAL`** directory, and had no non-inherited permissions. The default Security World Software installation gives everyone full control of the **`NFAST_KMLOCAL`** directory.

The current software sets an explicit ACL on new containers created by the CSP but does not alter permissions on previously created containers. The new permissions are as follows:

- **`READ`** access for **`EVERYONE`**
- **`FULL`** access for **`BUILTIN\Administrators`**

- for user containers: **FULL** access for the current user
- for machine containers: **FULL** access for **LOCALSYSTEM**

No action is required on the user's part to invoke the new behavior.

Symmetric keys in the nShield CSP are generated and stored entirely in software. These keys are not hardware protected and are no more secure than the corresponding keys in the Microsoft CSP.

The values of the **KP_PERMISSIONS** flags for hardware protected keys are enforced in software, except for **CRYPT_EXPORTABLE** which is ignored.

All CSP-generated, hardware-protected keys have ACLs that allow both signing and encryption. Hardware-protected keys that have been generated by the CSP are never exportable by the CSP; **CryptExportKey** always fails with a permissions error when called on such a key.

Container files and their associated key files can be moved freely between machines, as long as the user's SID is also valid on the destination machine. This is the case if the user in question is a domain user and both machines are on that domain. If the user's SID is not valid on the destination machine and keys are required to be shared between multiple machines, then the **cspimport** utility must be used to reassociate the Security World key file with the required destination container.

5.4 User interface issues

The nShield CSP supports hardware keys protected by either the module itself or by OCSs. Protecting keys with OCSs raises some user interface issues because the user interface needs to be displayed both at key-creation time and at key-loading time.

The choice of using module-protected keys or keys protected by OCSs is made in the install wizard. If, however, you generate keys protected by OCSs and then switch to module protection, then in most cases the keys protected by OCSs still require the user interface to be displayed in order to load them.

At key-generation time, if the **always display UI at key gen** flag is unset and an automatic Operator Card is present, the CSP uses the card set to protect the key, loading the shares automatically on all modules that contain a suitable card. (The flag is set using the install wizard.) Otherwise the CSP displays the user interface and blocks until the user interface is completed.

At key-loading time, if the key is protected by an automatic OCS, and the card set is present, then the key is loaded on all modules that contain a suitable card. Otherwise, the CSP displays the user interface and blocks until the user interface is completed; this requires the same steps as for key generation except for choosing the card set.

An automatic OCS means a card from a 1/*N* card set that is not protected by a pass phrase. At either time, the user interface is completed when the user has chosen a card set and the modules on which to load the key and has performed the card and pass phrase operations.

The CSP requires authorization to import keys (including public keys) and to generate keys when you have initialized your modules in the mode compatible with FIPS 140-2 level 3. This means that you must have a card from your current Security World in the slot when you attempt any of these operations, even if you are generating a module-protected key. If a card is not present, the operation blocks, and the CSP displays a user interface that prompts you to insert a card.

The CSP honors the `CRYPT_SILENT` flag to `CryptAcquireContext`. If this flag is passed in and the CSP would otherwise have to put up the user interface for any of the reasons in the two previous paragraphs, it fails with the appropriate error message.

If the CSP is being loaded from a service process (e.g. when used from within IIS or the main Certificate Authority process), then that process does not necessarily have access to the user's desktop. This means that any UI displayed by the CSP may not appear on an attended desktop (or at all), and the underlying operation may well time out.

If this is the case (and you are not using the `CRYPT_SILENT` flag, for whatever reason), we recommend that either you do not use OCS-protected keys or you use an automatic card set, so that the CSP does not display the UI.

5.5 Key counting

The nShield CSP supports the `PP_CRYPT_COUNT_KEY_USE` parameter to CryptAcquireContext as long as the module with NVRAM is attached. Setting this parameter to a nonzero value causes all keys generated from that point to have nonvolatile use counters. The counter persists until CryptReleaseContext is called or until the `PP_CRYPT_COUNT_KEY_USE` parameter is reset to `0`.

ℹ Key counting is not directly supported by end-user applications such as IIS . It is only supported by Microsoft Certificate Services under Windows 2003 and later. However, it is possible to create a certificate that uses a key counter in cases where key counting is not directly supported. For more information about key counting, see the User Guide.

ℹ Key counting is not supported in HSM Pool mode.

Keys that have counters can only be loaded on one module at a time. The key-generation and key-loading functions enforce this behavior. When you generate these keys, you must present your Administrator Cards in order to authorize the creation of the new NVRAM area.

ℹ You must not insert your Administrator Cards in an untrusted host.

To minimize the exposure of the Security Officer root key ($\mathbf{K}_{NSO}$) when you generate a key with key counting enabled, you should create the Security World with an NVRAM delegation key that requires the presentation of fewer Administrative Cards than are required to load $\mathbf{K}_{NSO}$.

If you reinitialize your module for any reason, all the NVRAM areas on that module are erased. You must then use `cspnvfix` to recreate the NVRAM areas for all the keys that have counters.

5.6 NVRAM-stored keys

The nShield CSP now supports creating keys protected by the module NVRAM. The `PP_NO_HOST_STORAGE` parameter to `CryptAcquireContext` is supported as long as the module with NVRAM is attached. Setting this parameter to a nonzero value causes all keys generated from that point to be generated with blobs in NVRAM. The counter persists until CryptReleaseContext is called or until the `PP_NO_HOST_STORAGE` parameter is reset to `0`.

The method of creating NVRAM-stored keys is very similar to the method of creating keys with NVRAM counters:

1. call **`CryptAcquireContext`** to get a handle to a container.
2. call **`CryptSetProvParam`** and set the **`PP_NO_HOST_STORAGE`** property to a non-zero value.

This causes any keys generated with that container handle to be generated with blobs in NVRAM until either of the following occurs:

- **`CryptReleaseContext`** is called with that container handle
- **`CryptSetProvParam`** is called to set **`PP_NO_HOST_STORAGE`** to zero

Creating NVRAM-stored keys requires insertion of the ACS quorum for NVRAM, in the same way as creating key counted keys.

`PP_NO_HOST_STORAGE` is a new value and will be set in the **`wincrypt.h`** header file in future versions of the Microsoft Platform SDK. The following example code can be used until then to define the value correctly:

```
#ifndef PP_NO_HOST_STORAGE
#define PP_NO_HOST_STORAGE 44
#endif
```

This feature is only available to users writing CAPI code directly. To use a NVRAM-stored key in a client application (for example IIS or the Microsoft Certificate Authority), first create the key with the **`keytst`** command-line tool, and then transfer the key across to the required container with the **`cspimport`** utility.

Also, the **`keytst`** and **`csptest`** utilities have gained an extra command-line parameter. **`keytst --help`** now gives output containing the following information:

```
Key creation flags (only valid with -cx or -cs):
-e, --export                Create the key(s) with the 'exportable' bit set.
  -L, --length=BITLEN       Specify the new key length (default = 1024).
  -C, --counter             Create key counters (if supported).
  -K, --kitb                Create NVRAM-stored key(s) (if supported).
```

ℹ The **`-C`** and **`-K`** options require you to insert your ACS.

The command **`csptest --help`** outputs the following usage message:

```
Program options:
  -f, --flood               Run a continuous signature test.
  -d, --dsa                 Use DSA signatures rather than RSA signatures.
  -m, --ms                  Use the MS AES provider rather than nCipher's one
                              (possibly with modexp offload).
  -C, --counters            Generate keys with counters (needs NVRAM and ACS).
  -K, --kitb                Generate keys using KITB (needs NVRAM and ACS).
```

The **`csputils`** utility displays the NVRAM status of keys using the **`--detail`** option.

5.7 CSP setup and utilities

nCipher provides a CSP installation wizard that creates a new Security World, loads an existing Security World, or sets up the modexp offload DLL. The CSP installation wizard also generates new OCSs and the set-up parameters of the CSP, and allows HSM Pool mode to be configured for CAPI. However, the installation wizard is not suitable for complex Security World setups. If you require more flexibility than the CSP install wizard provides, use **`new-world`** and **`createocs`**, or **`KeySafe`**, to create your Security World.

The standard Security World utility **`nfkmverify`** should be used to check the security of all stored keys in the Security World; **`nfkminfo`**, **`nfkmcheck`** and other standard utilities can also be used to assist in this process.

Additionally, nCipher provides some CSP-specific command-line utilities:

- **`csputils`** provides an overview of the containers and keys present and also tells you the values of the counters for key-counted keys
- **`cspcheck`** is for use alongside **`nfkmcheck`**
- **`cspimport`** allows you to move keys between containers or to import a pre-generated NFKM key into a container
- **`cspmigrate`** allows you to move the CSP container information from the registry into the Security World
- **`cspnvfix`** allows you to regenerate NVRAM areas in modules where these have been erased (for example, by reinitialization)
- **`csptest`** is a general test utility that can be used to list the capabilities of installed nShield and Microsoft CSPs or to perform a soak test
- **`keytst`** allows you to generate containers and keys and also to list the available containers
- **`configure-csp-poolmode`** allows you to configure HSM Pool mode for the nCipher CAPI CSP without using the CSP wizard.

For more information about these utilities, see the *User Guide* for your HSM.

6 Microsoft CNG

Cryptography API: Next Generation (CNG) is the successor to the Microsoft Crypto API (CAPI) and its long-term replacement. The Security World Software implementation of Microsoft CNG is supported on Microsoft Windows Windows Server 2008 (for both x86 and x64 architectures) and later releases, including Windows Server 2012. The nShield CNG providers offer the benefits of hardware-based encryption accessed through the standard Microsoft API, and support the National Security Agency (NSA) classified Suite B algorithms.

Before using the nShield CNG providers, run the nShield CNG Configuration Wizard to:

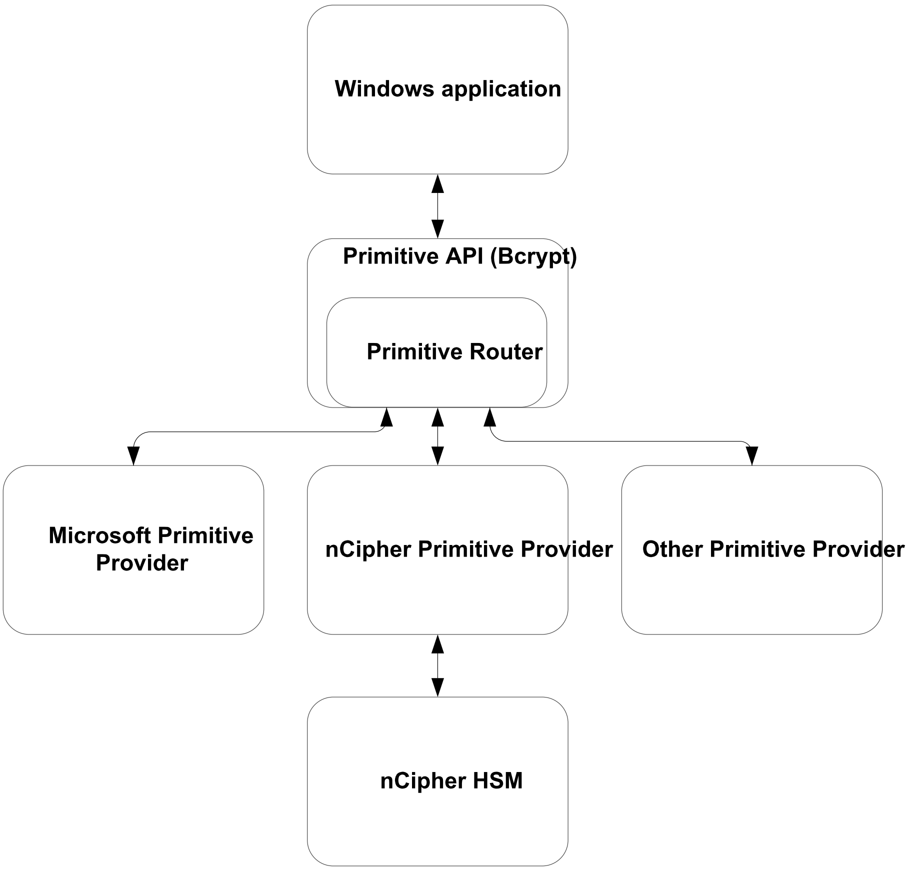
- configure HSM Pool mode for CNG as required
- create a new Security World or specify an existing Security World to use
- register the nShield CNG providers
- configure the nShield CNG providers as default CNG providers for specific tasks.

This chapter describes the features and implementation details of the nShield CNG providers. For more information, see the Microsoft CNG documentation: http://msdn2.microsoft.com/en-us/library/aa376210.aspx.

6.1 CNG architecture overview

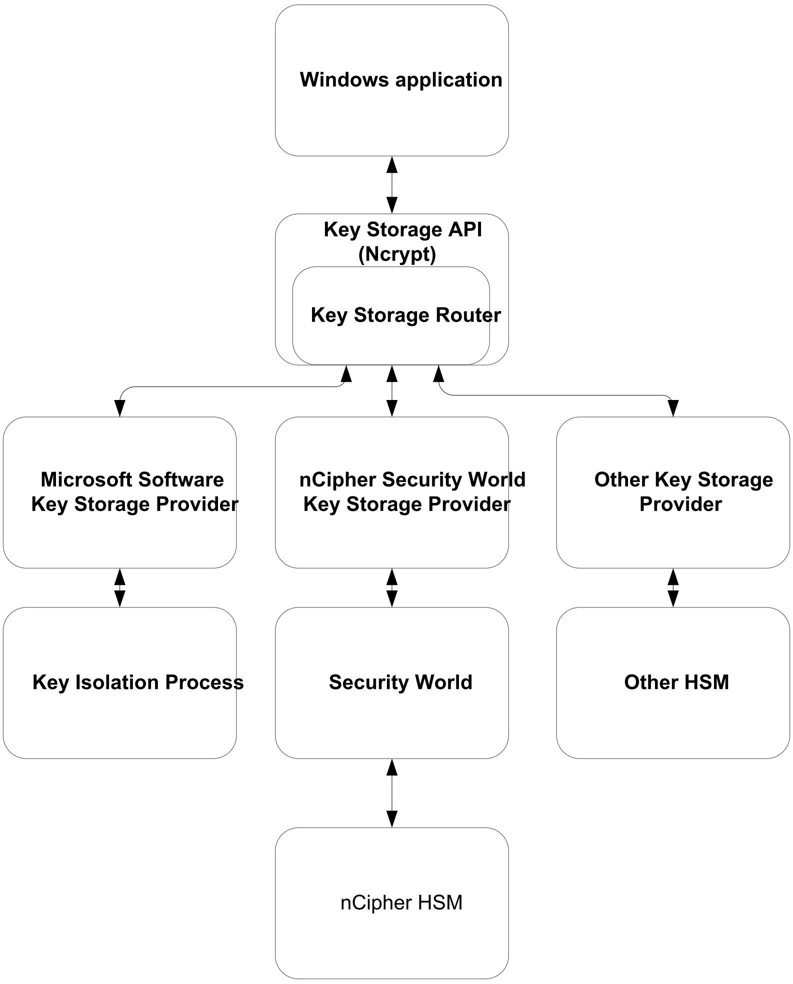
CNG handles cryptographic primitives and key storage through separate APIs. In both cases a Windows application contacts a router, which forwards the cryptographic operation to the provider that is configured to handle the request. For an illustration of communication between the architecture layers for cryptographic primitives, see Figure 5.

Figure 5. CNG primitives



For an illustration of communication between the architecture layers for cryptographic key storage, see Figure 6.

Figure 6. Key storage



6.2 Supported algorithms for CNG

This section lists the National Security Agency (NSA) classified Suite B algorithms supported by the nShield CNG providers.

The MQV algorithm is not supported by the nShield CNG providers.

Some mechanisms may be restricted from use in Security Worlds conforming to FIPS 140-2 Level 3. See the *User Guide* for your HSM for more information.

6.2.1 Signature interfaces (key signing)

Interface name	*Type of support*
RSA PKCS#1 v1	Hardware
RSA PSS	
DSA	
ECDSA_P224	
ECDSA_P256	
ECDSA_P384	
ECDSA_P521	

ℹ Hashes used with ECDSA must be of the same length or shorter than the curve itself. If you attempt to use a hash longer than the curve the operation returns **NOT_SUPPORTED**. In FIPS 140-2 level 3 Security Worlds, curves must be of an approved type and length.

6.2.2 Hashes

Hash name	*Type of support*
SHA1	Hardware (HMAC only)/software
SHA256	
SHA384	
SHA512	
SHA224	Hardware (HMAC only, requires firmware version 2.33.60 or later)/software
MD5	Hardware (HMAC only)/software

6.2.3 Asymmetric encryption

Algorithm name	*Type of support*
RSA Raw (NCRYPT_NO_PADDING_FLAG)	Hardware
RSA PKCS#1 v1 (NCRYPT_PAD_PKCS1_FLAG)	
RSA OAEP (NCRYPT_PAD_OAEP_FLAG)	

6.2.4 Symmetric encryption

Algorithm name	*Type of support*
RC4	Hardware and Software
AES ECB,CBC	
DES ECB,CBC	
3DES ECB,CBC	
3DES_112 ECB,CBC	

6.2.5 Key exchange

Protocol name	*Type of support*
DH	Hardware
ECDH_P224	
ECDH_P256	
ECDH_P348	
ECDH_P521	

ℹ Elliptic curve cryptography algorithms must be enabled before use. Use the `fet` command-line utility with an appropriate certificate to enable a purchased feature. If you enable the elliptic curve feature on your modules after you first register the CNG providers, you must run the configuration wizard again for the elliptic curve algorithm providers to be registered. For more information about registering the CNG providers, see the *User Guide* for your HSM.

6.2.6 Random Number Generation

Name	*Type of support*
RNG	Hardware

6.3 Key authorization for CNG

When an application needs keys that are protected by an Operator Card Set or a Softcard, a user interface is invoked to prompt the application user to insert the smart card and/or enter appropriate pass phrases.

ℹ The user interface prompt is not provided if your application is working in silent mode. The nShield CNG providers attempt to load the required authorization (for example, from an Operator Card that has already been inserted) but fail if no authorization can be found. For more information about silent mode, refer to the documentation of the CNG Key Storage Functions at: http://msdn2.microsoft.com/en-us/library/aa376208.aspx.

When the CNG application is running in Session 0 (i.e. loaded by a Windows service), the user interface is provided by an agent process **nShield Service Agent** that is started when the user logs in. This agent, when running, is shown in the Windows System Tray. All user interaction requests from a CNG application running in Session 0 cause dialogs to be raised by the agent allowing the user to select cardsets, modules and enter passphrases. The interaction with the user is functionally identical to that described in this section.

There can only be one instance of the agent running (indicated by a blue globe in the Tray Notification area in the toolbar). Attempts to start a second instance will fail with a **CreateNamedPipe** error. If the agent is not running, attempts to invoke dialogs through it will fail and this is logged in the Windows Event Log. It can be restarted by logging off and on or by explicitly executing either `%NFAST_HOME%\bin\nShield_service_agent64.exe` or `%NFAST_HOME%\bin\nShield_service_agent.exe`. On 64 bit platforms either of these can be used irrespective of the bit size of the underlying application.

For more information about auto-loadable card sets and the considerations of silent mode, see Figure 7.

You define key protection and authorization settings with the CNG Configuration Wizard on the **Key Protection Setup** screen. For more information about the CNG Configuration Wizard, see the *User Guide* for your HSM.

The options on this screen that are relevant to key protection and authorization are:

- **Module protection**

  Select this option to make keys module protected by default.

- **Softcard Protection**

  Select this option to generate new keys with a particular Softcard by default.

- **Operator Card Set protection**

  Select this option to generate new keys with a particular Operator Card Set by default.

- **Allow any protection method to be selected in the GUI when generating**

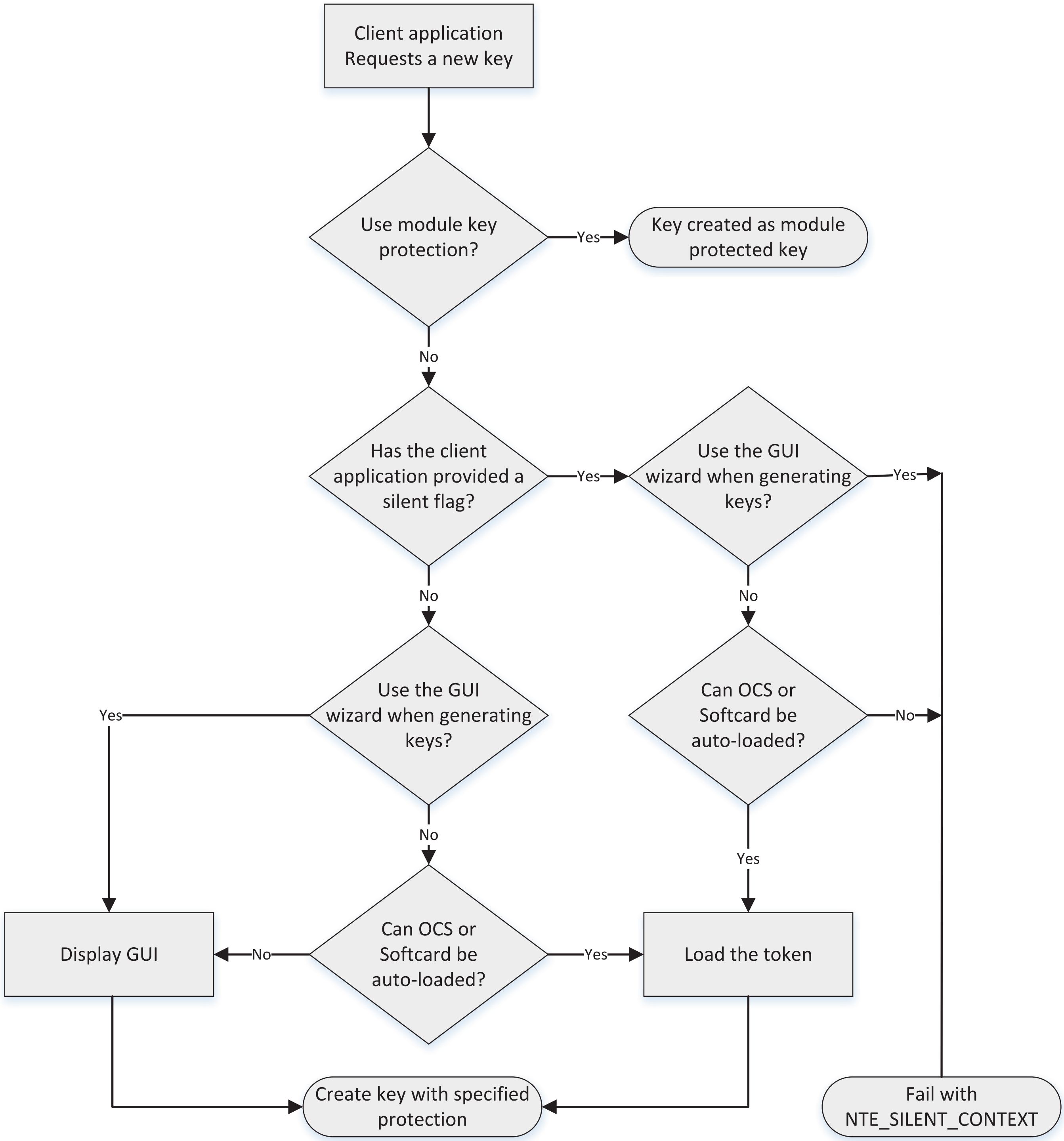
  Select this option to defer selection of the key protection until the key is generated. When generating a key, the choice between Module protection, or protection with an existing Softcard or Operator Card Set, will be offered.

If you select Softcard or Operator Card Set protection, you will be offered the choice between selecting an existing protection token and creating a new one on the next page.

The CNG Configuration Wizard can be re-run to change the default protection. Existing keys that were generated with a different protection can still be loaded even if they don't match the protection that was selected in the wizard.

The nShield GUI is never enabled for calls with a valid **Silent** option. If the **Use the GUI wizard..** option is selected, and the providers have been passed the **Silent** option, key generation will always fail. For Softcard and Operator Card Set protection, **Silent** mode will work only if the Softcard or Operator Card Set can be autoloaded without prompting for user interaction or passphrase entry.

Figure 7. Key authorization requests


Client application Requests a new key
Use module key protection?
Yes
Key created as module protected key
No
Has the client application provided a silent flag?
Yes
Use the GUI wizard when generating keys?
Yes
No
Use the GUI wizard when generating keys?
Yes
No
Can OCS or Softcard be auto-loaded?
No
Yes
Display GUI
No
Can OCS or Softcard be auto-loaded?
Yes
Load the token
Create key with specified protection
Fail with NTE_SILENT_CONTEXT

FIPS 140-2 level 3 environments always require card authorization for key creation. When using the CNG Primitive Functions the user is not prompted to provide card authorization, but the request fails if no card is provided.

The key storage providers always respect calls made with the `Silent` option. Primitive providers never display a user interface.

Applications may have a mechanism to disable silent mode operation, thereby allowing appropriate pass phrases to be entered. Ensure that you configure applications to use an appropriate level of key protection. For example, in Microsoft Certificate Services, you must select the **Use strong private key protection features provided by the CSP** option to disable silent mode operation.

6.4 Key use counting

You can configure the CNG provider to count the number of times a key is used. Use this functionality, for example, to retire a key after a set number of uses, or for auditing purposes.

Key counting is not supported in HSM Pool mode.

To enable key use counting in the Security World Key Storage Provider, call **NCryptSetProperty** with **NCRYPT_USE_COUNT_ENABLED_PROPERTY** on the provider handle. Alternatively, to override the behavior of third-party software that would not otherwise provide the user with the option to enable key use counting, use one of the following methods:

- set the environment variable **NCCNG_USE_COUNT_ENABLED** to **1**
- set the registry key **Software\nCipher\CryptoNG\UseCountEnabled** to **1**

Keys created while the provider has key use counting enabled continue to have their use counts incremented, regardless of the state of the provider's handle. Key use counts are not recorded for keys created while the **NCRYPT_USE_COUNT_ENABLED_PROPERTY** is disabled on the provider handle.

Because the key counter is a 64-bit area in a specific module's NVRAM, the counted keys are specific to a single module. When a key is created you are prompted to specify which module to use, unless there is only one module in the Security World, or **preload** was used to preload authorization from an ACS on only one module.

The key counter is incremented each time a private key is used to:

- sign
- decrypt
- negotiate a secret agreement.

To test the performance of keys with counters, run the **cngsoak** command with the **-C** option:

```
cngsoak -C --sign --length=1024
```

To view the current key use count for keys, run the **cnglist** command with the **--list-keys** and **--verbose** options:

```
cnglist --list-keys --verbose
```

6.5 Using CAPI keys in CNG

We now provide the capability to use keys generated by CAPI in CNG applications. This is provided through the standard **NCryptOpenKey** CNG API call. Passing either **AT_SIGNATURE** or **AT_KEYEXCHANGE** as the **dwLegacyKeySpec** parameter and the CAPI container name as the **pszKeyName** parameter will invoke this mode of operation. The CAPI key will be loaded into the CNG provider and will behave as if it was a CNG key. Any key authorization required will be handled with a user interface being invoked to prompt the application user to insert the smart card or enter appropriate pass phrases. There is support for Key Usage and Key Counting properties.

The CNG application has to be written such that it calls **NCryptOpenKey** to open a CAPI key explicitly.

6.6 Utilities for CNG

Use the **nfkmverify** command-line utility to check the security of all stored keys in the Security World. Use **nfkminfo**, **nfkmcheck**, and other command-line utilities to assist in this process. For more information about these command-line utilities, see the *User Guide* for your HSM.

The following table lists the utilities specific to the nCipher CNG CSP:

x86	x64	Utility description
cngimport.exe	**cngimport.exe**	This key migration utility is used to migrate Security World, CAPI, and CNG keys to the Security World Key Storage Provider.
cnginstall.exe	**cnginstall64.exe**	This utility is the nCipher CNG CSP installer. Only use this utility to remove or reinstall the provider DLLs and associated registry entries manually.
cnglist.exe	**cnglist.exe**	This utility lists information about CNG CSP.
cngregister.exe	**cngregister.exe**	This is the nCipher CNG CSP registration utility. You can use it to unregister and re-register the nCipher providers manually.
cngsoak.exe	**cngsoak64.exe**	This utility is the nCipher CNG soak tool. You can use it to evaluate the performance of signing, key exchange, and key generation using a user-defined number of threads.
ncsvcdep.exe	**ncsvcdep.exe**	This utility is the service dependency tool. You can configure some service based applications, such as Microsoft Certificate Services and IIS, to use the nCipher CNG CSP. The nShield Service dependency tool allows you to add the nFast Server to the dependency list of such services.
configure-csp-poolmode	**configure-csp-poolmode64**	This utility allows you to configure HSM Pool mode for the nCipher CNG CSP without using the CNG wizard.

For more information about the command-line utilities, see the *User Guide* for your HSM.

6.7 Environment variables that control CNG protection options

A set of environment variables are supported for controlling CNG protection options on a per-application basis. These variables are documented here to facilitate more complicated deployments, but it should be noted that they are liable to change between releases.

Environment Variable	Description
`NCCNG_PIN`	Passphrase for Softcard. This enables the passphrase to be specified programmatically rather than through the GUI passphrase prompt. Note: This can expose your passphrase. ℹ It is recommended that this be set in a context where the passphrase will be visible only to the user or service that should have access to this passphrase. It should **not** be set as a machine-wide environment variable.
`NCCNG_USE_MODULE_KEYS`	• If set to 1, module protection will be used for new keys that are generated. • If set to 0, the **`NCCNG_PROTECTION_TOKEN`** environment variable controls the protection option used.
`NCCNG_PROTECTION_TOKEN`	If **`NCCNG_USE_MODULE_KEYS`** is set to 0 (or a protection option other than module key protection or HSM pool mode was selected in the wizard) this environment variable enables the protection token to be specified for new keys that are generated. • If set to **`softcard:HASH`** the Softcard with the specified hash will be used. • If set to **`cardset:HASH`** the OCS with the specified hash will be used. • If set to anything else (e.g. wizard), the GUI key protection wizard will be used. The HASH for Softcard or OCS protections refers to its Security World hash in hexadecimal, which can be identified using **`nfkminfo -s`** for softcards or **`nfkminfo -c`** for OCS.
`NCCNG_ALWAYS_USE_AGENT`	By default, if a CNG provider must display GUI, it will display it in the calling application if not in Session 0, and in the nShield Service Agent if running in Session 0 (e.g. running as a service). Setting **`NCCNG_ALWAYS_USE_AGENT`** to 1 forces CNG GUI prompts to always be displayed in the nShield Service Agent regardless of whether it is running in Session 0.

7 nCipherKM JCA/JCE CSP

The nCipherKM JCA/JCE CSP (Cryptographic Service Provider) allows Java applications and services to access the secure cryptographic operations and key management provided by nCipher hardware. This provider is used with the standard JCE (Java Cryptographic Extension) programming interface.

To use the nCipherKM JCA/JCE CSP, you must install:

- the **`javasp Java Support (including KeySafe)`** bundle
- the **`jcecsp nCipherKM JCA/JCE provider classes`** component.

For more information about the bundles and components supplied on your Security World Software installation media, see the User Guide.

The following versions of Java have been tested to work with, and are supported by, your nCipher Security World Software:

- Java6 (or Java 1.6x)
- Java7 (or Java 1.7x)
- Java8 (or Java 1.8x).

We recommed that you ensure Java is installed before you install the Security World Software. The Java executable must be on your system path

If you can do so, please use the latest Java version currently supported by nCipher that is compatible with your requirements. Java versions before those shown are no longer supported. If you are maintaining older Java versions for legacy reasons, and need compatibility with current nCipher software, please contact nCipher Support.

To install Java you may need installation packages specific to your operating system, which may depend on other pre-installed packages to be able to work.

Suggested links from which you may download Java software as appropriate for your operating system are:

Operating System	Download site
AIX	http://www.ibm.com/developerworks/systems/library/es-JavaOnAix_install.html
HPUX	https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXJAVAHOME
various	http://www.oracle.com/technetwork/java/index.html
various	http://www.oracle.com/technetwork/java/all-142825.html

ℹ Detailed documentation for the JCE interface can be found on the Oracle Technology web page https://docs.oracle.com/javase/7/docs/technotes/guides/security/crypto/CryptoSpec.html.

ℹ Softcards are not supported for use with the nCipherKM JCA/JCE CSP in Security Worlds that are compliant with FIPS 140-2 level 3.

7.1 Installing the nCipherKM JCA/JCE CSP

To install the nCipherKM JCA/JCE CSP:

1. In the hardserver configuration file, ensure that:
   - **`priv_port`** (the port on which the hardserver listens for local privileged TCP connections) is set to 9001
   - **`nonpriv_port`** (the port on which the hardserver listens for local nonprivileged TCP connections) is set to 9000.

   If you need to change either or both of these port settings, you restart the hardserver before continuing the nCipherKM JCA/JCE CSP installation process. For more information, see the User Guide.

2. Copy the **`nCipherKM.jar`** file to the extensions folder of your local Java Virtual Machine installation from the following directory:
   - Windows: *%NFAST_HOME%*`\java\classes`
   - Unix-based: `/opt/nfast/java/classes`

   The location of the extensions folder depends on the type of your local Java Virtual Machine (JVM) installation:

JVM type	Extensions folder
Java Developer Kit (JDK)	Windows: *%JAVA_HOME%*`\jre\lib\ext` Unix-based: *$JAVA_HOME*`/jre/lib/ext`
Java Runtime Environment (JRE)	Windows: *%JAVA_HOME%*`\lib\ext` Unix-based: *$JAVA_HOME*`/lib/ext`

   In these paths, *%JAVA_HOME%* (Windows) or *$JAVA_HOME* (Unix-based) is the home directory of the Java installation (commonly specified in the **`JAVA_HOME`** environment variable).

3. Add *%JAVA_HOME%*`\bin` (Windows) or *$JAVA_HOME*`/bin` (Unix-based) to your **`PATH`** system variable.

4. Install the unlimited strength JCE jurisdiction policy files that are appropriate to your version of Java.

   The Java Virtual Machine imposes limits on the cryptographic strength that may be used by default with JCE providers. Replace the default policy configuration files with the unlimited strength policy files.

   To install the unlimited strength JCE jurisdiction policy files:

   a. If necessary, download the archive containing the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files from your Java Virtual Machine vendor's Web site. Be sure to download a file appropriate for your version of Java.

      ℹ The Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files are covered and controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. We recommend that you take legal advice before downloading these files from your Java Virtual Machine vendor.

   b. Extract the files **`local_policy.jar`** and **`US_export_policy.jar`** from Java Virtual Machine vendor's Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy File archive.

   c. Copy the extracted files **`local_policy.jar`** and **`US_export_policy.jar`** into the security directory for your local Java Virtual Machine (JVM) installation:

JVM type	Extensions folder
Java Developer Kit (JDK)	Windows: *%JAVA_HOME%*`/jre\lib\security` Unix-based: *$JAVA_HOME*`/jre/lib/security`
Java Runtime Environment (JRE)	Windows: *%JAVA_HOME%*`\lib\security` Unix-based: *$JAVA_HOME*`/lib/security`

In these paths, *%JAVA_HOME%* (Windows) or *$JAVA_HOME* (Unix-based) is the home directory of the Java installation (commonly specified in the **`JAVA_HOME`** environment variable).

ℹ Copying the files **`local_policy.jar`** and **`US_export_policy.jar`** into the appropriate folder must overwrite any existing files with the same names.

5. Add the nCipherKM provider to the Java security configuration file **`java.security`** (located in the security directory for your local Java Virtual Machine (JVM) installation).

   The **`java.security`** file contains list of providers in preference order that is used by the Java Virtual Machine to decide from which provider to request a mechanism instance. Ensure that the nCipherKM provider is registered in the first position in this list, as shown in the following example:

   ```
   #
   # List of providers and their preference orders (see above):
   #
   security.provider.1=com.ncipher.provider.km.nCipherKM
   security.provider.2=sun.security.provider.Sun
   security.provider.3=sun.security.rsa.SunRsaSign
   security.provider.4=com.sun.net.ssl.internal.ssl.Provider
   security.provider.5=com.sun.crypto.provider.SunJCE
   security.provider.6=sun.security.jgss.SunProvider
   security.provider.7=com.sun.security.sasl.Provider
   ```

   Placing the nCipherKM provider first in the list permits the nCipherKM provider's algorithms to override the algorithms that would be implemented by any other providers (except in cases where you explicitly request another provider name).

   The nCipherKM provider cannot serve requests required for the SSL classes unless it is in the first position in the list of providers.

   Do not change the relative order of the other providers in the list.

   If you add the nCipherKM provider as **`security.provider.1`**, ensure that the subsequent providers are re-numbered correctly. Ensure you do not list multiple providers with the same number (for example, ensure your list of providers does not include two instances of **`security.provider.1`**, both **`com.ncipher.provider.km.nCipherKM`** and another provider).

6. Save your updates to the file **`java.security`**.

   When you have installed the nCipherKM JCA/JCE CSP, you must have created a Security World before you can test or use it. For more information about creating a Security World, see the User Guide.

   If you have a Java Enterprise Edition Application Server running, you must restart it before the installed nCipherKM provider is loaded into the Application Server virtual machine and ready for use.

7.1.1 Testing the nCipherKM JCA/JCE CSP installation

After installation, you can test that the nCipherKM JCA/JCE CSP is functioning correctly by running the command:

```
java com.ncipher.provider.InstallationTest
```

For this command to work, you must have added *%JAVA_HOME%* (Windows) or *$JAVA_HOME* (Unix-based) to your **`PATH`** system variable.

If the nCipherKM JCA/JCE CSP is functioning correctly, output from this command has the following form:

```
Installed providers:
1: nCipherKM
2: SUN
3: SunRsaSign
4: SunJSSE
5: SunJCE
6: SunJGSS
7: SunSASL
Unlimited strength jurisdiction files are installed.
The nCipher provider is correctly installed.
nCipher JCE services:
Alg.Alias.Cipher.1.2.840.113549.1.1.1
Alg.Alias.Cipher.1.2.840.113549.3.4
Alg.Alias.Cipher.AES
Alg.Alias.Cipher.DES3
....
```

If the **`nCipherKM`** provider is installed but is not registered at the top of the providers list in the **`java.security`** file, the **`InstallationTest`** command produces output that includes the message:

```
The nCipher provider is installed, but is not registered at
the top of the providers list in the java.security file. See
the user guide for more information about the recommended
system configuration.
```

In such a case, edit the **`java.security`** file (located in the security directory for your local JVM installation) so that the nCipherKM provider is registered in the first position in that file's list of providers. For more information about the **`java.security`** file, see *Installing the nCipherKM JCA/JCE CSP* on page 91.

If the nCipherKM provider is not installed at all, or you have not created a Security World, or if you have not configured ports correctly in the hardserver configuration file, the **`InstallationTest`** command produces output that includes the message:

```
The nCipher provider is not correctly installed.
```

In such case:

- Check that you have configured ports correctly, as described in *Installing the nCipherKM JCA/JCE CSP* on page 91. For more information about hardserver configuration file settings, see the User Guide.
- Check that you have created a Security World. If you have not created a Security World, create a Security World. For more information, see the User Guide.

- If you have already created a Security World, repeat the nCipherKM JCA/JCE CSP installation process as described in *Installing the nCipherKM JCA/JCE CSP* on page 91.

After making any changes to the nCipherKM JCA/JCE CSP installation, run the **`InstallationTest`** command again and check the output.

Whether or not the nCipherKM provider is correctly installed, if the unlimited strength jurisdiction files are not installed or (not correctly installed), the **`InstallationTest`** command produces output that includes the message:

```
Unlimited strength jurisdiction files are NOT installed.
```

ℹ The **`InstallationTest`** command can only detect this situation if you are using JRE/JDK version 1.6 or later.

This message means that, because the Java Virtual Machine imposes limits on the cryptographic strength that you can use by default with JCE providers, you must replace the default policy configuration files with the unlimited strength policy files. For information about how to install the unlimited strength jurisdiction files, see *Installing the nCipherKM JCA/JCE CSP* on page 91.

7.2 System properties

You can use system properties to control the provider. You set system properties when starting the Java Virtual Machine using a command such as:

```
java -Dproperty=value MyJavaApplication
```

In this example command, *property* represents any system property, *value* represents the value set for that property, and *MyJavaApplication* is the name of the Java application you are starting. You can set multiple system properties in a single command, for example:

```
java -Dprotect=module -DignorePassphrase=true MyJavaApplication
```

The available system properties and their functions as controlled by setting different values for a property are described in the following table:

Property	Function for different values
`JCECSP_DEBUG`	This property is a bit mask for which different values specify different debugging functions; the default value is **`0`**. For details about the effects of setting different values for this property, see *JCECSP_DEBUG property values* on page 97.

Property	Function for different values
`JCECSP_DEBUGFILE`	This property specifies a path to the file to which logging output is to be written. Set this property if the **`JCECSP_DEBUG`** property is set to a value other than the default of **`0`**. For details about the effects of setting different values for this property, see *JCECSP_DEBUG property values* on page *97*. In a production environment, we recommend that you disable debug logging to prevent sensitive information being made available to an attacker.
`protect`	This property specifies the type of protection to be used for key generation and nCipherKM KeyStore instances. You can set the value of this property to one of **`module`**, **`softcard:`***IDENT* or **`cardset`**. OCS protection (**`cardset`**) uses the card from the first slot of the first usable hardware security module. To find the logical token hash *IDENT* of a softcard, run the command **`nfkminfo --softcard-list`**.
`module`	This property lets you override the default module and select a specific module to use for module and OCS protection. Set the value of this property as the ESN of the module you want to use.
`slot`	This property lets you override the default slot for OCS-protection and select a specific slot to use. Set this the value of this property as the number of the slot you want to use.
`ignorePassphrase`	If the value of this property is set to **`true`**, the nCipherKM provider ignores the pass phrase provided in its KeyStore implementation. This feature is included to allow the Oracle or IBM **`keytool`** utilities to be used with module-protected keys. The **`keytool`** utilities require a pass phrase be provided; setting this property allows a dummy pass phrase to be used.
`seeintegname`	Setting the value of this property to the name of an SEE integrity key causes the provider to generate SEE application keys. These keys may only be used by an SEE application signed with the named key.
`com.ncipher.provider.announcemode`	The default value for this property is **`auto`**, which uses firmware auto-detection to disable algorithms in the provider that cannot be supported across all installed modules. Setting the value of this property to **`on`** forces the provider to advertise all mechanisms at start-up. Setting the value of this property to **`off`** forces the provider to advertise no mechanisms at start-up.
`com.ncipher.provider.enable`	For the value of this property, you supply a comma-separated list of mechanism names that are to be forced on, regardless of the announce mode selected.

Property	Function for different values
`com.ncipher.provider.disable`	For the value of this property, you supply a comma-separated list of mechanism names that are to be forced off, regardless of the announce mode selected. Any mechanism supplied in the value for the `com.ncipher.provider.disable` property overrides the same mechanism if it is supplied in the value for the `com.ncipher.provider.enable` property.

7.2.1 JCECSP_DEBUG property values

The **JCECSP_DEBUG** system property is a bit mask for which you can set different values to control the debugging functions. The following table describes the effects of different values that you can set for this property:

JCECSP_DEBUG value	Function
0	If this property has no bits set, no debugging information is reported. This is the default setting.
1	If this property has the bit 1 set, minimal debugging information (for example, version information and critical errors) is reported.
2	If this property has the bit 2 set, comprehensive debugging information is reported.
4	If this property has the bit 3 set, debugging information relating to creation and destruction of memory and module resources is reported.
8	If this property has the bit 4 set, **debugFunc** and **debugFuncEnd** generate debugging information for functions that call them.
16	If this property has the bit 5 set, **debugFunc** and **debugFuncEnd** display the values for all the arguments that are passed in to them.
32	If this property has the bit 6 set, context information is reported with each debugging message (for example, the **ThreadID** and the current time.
64	If this property has the bit 7 set, the time elapsed during each logged function is calculated, and information on the number of times a function is called and by which function it was called is reported.
128	If this property has the bit 8 set, debugging information for NFJAVA is reported in the debugging file.
256	If this property has the bit 9 set, the call stack is printed for every debug message.

To set multiple logging functions, add up the **JCECSP_DEBUG** values for the debugging functions you want to set, and specify the total as the value for **JCECSP_DEBUG**. For example, if you want to set the debugging to use both function tracing (bit 4) and function tracing with parameters (bit 5), add the **JCECSP_DEBUG** values shown in the table for these debugging functions (**8** + **16** = 24) and specify this total (**24**) as the value to use for **JCECSP_DEBUG**.

7.3 Compatibility

The nCipherKM JCA/JCE CSP supports both module-protected keys and OCS-protected keys. The CSP currently supports 1/*N* OCSs and a single protection type for each nCipherKM JCE KeyStore.

You can use the nCipherKM JCA/JCE CSP with Security Worlds that comply with FIPS 140-2 at either level 2 or level 3.

In a Security World that complies with FIPS 140-2 level 3, it is not possible to import keys generated by other JCE providers.

The nCipherKM JCA/JCE CSP supports load-sharing for keys that are stored in the nCipherKM KeyStore. This feature allows a server to spread the load of cryptographic operations across multiple connected modules, providing greater scalability.

We recommend that you use load-sharing unless you have existing code that is designed to run with multiple modules. To share keys with load-sharing, you must create a 1/*N* OCS with at least as many cards as you have modules. All the cards in the OCS must have the same pass phrase.

Keys generated or imported by the nCipherKM JCA/JCE CSP are not recorded into the Security World until:

1. The key is added to an nCipherKM KeyStore (by using a call to **`setKeyEntry()`** or **`setCertificateEntry()`**).
2. That nCipherKM KeyStore is then stored (by using a call to **`store()`**).

The pass phrase used with the KeyStore must be the pass phrase of the card from the OCS that protects the keys in the KeyStore.

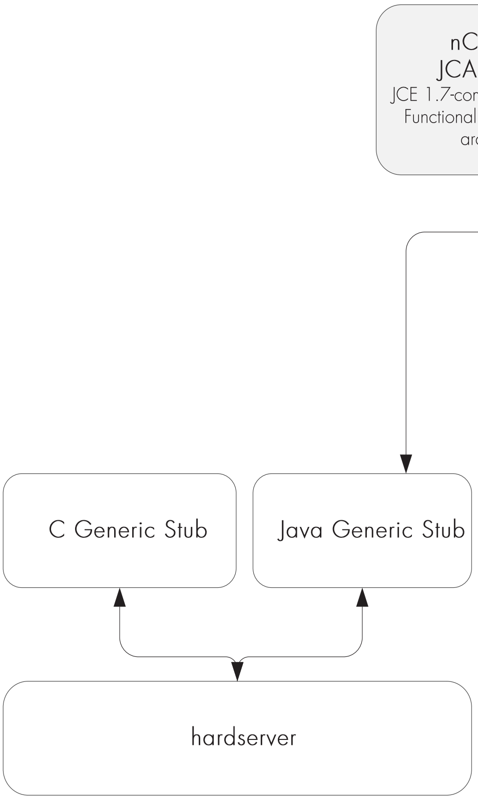
7.4 Architecture

The nCipherKM JCA/JCE CSP implements its functionality using two underlying nShield APIs:

- the KM Java library (**`kmjava`**)
- the Java Generic Stub (**`nfjava`**).

These libraries relay commands generated by the JCE provider to the underlying hardserver and modules.

Figure 8. nCipherKM JCA/JCE CSP architecture



7.5 Available functions

The module firmware automatically detects which algorithms it can support. These algorithms are advertised when the provider first starts up. The provider conservatively advertises only those mechanisms that are supported by all installed modules in the system.

Certain algorithms are not supported by older versions of firmware. We recommend that you ensure that your module is upgraded to the most recent version of firmware appropriate for your environment.

Cipher	Cipher mode						Padding type							
	CBC	CFB	CTR	ECB	OFB	GCM	ANSI X9.23	ISO 10126	ISO 7816	None	OAEP	PKCS #1	PKCS #5	Zero byte
AESWrap				X						X				
ArcFour														
Blowfish	X	X	X	X	X		X	X	X	X			X	X
CAST256	X	X	X	X	X		X	X	X	X			X	X
Blowfish	X	X	X	X	X		X	X	X	X			X	X

Cipher	Cipher mode						Padding type							
	CBC	CFB	CTR	ECB	OFB	GCM	ANSI X9.23	ISO 10126	ISO 7816	None	OAEP	PKCS #1	PKCS #5	Zero byte
CAST	X	X	X	X	X		X	X	X	X			X	X
DES2	X	X	X	X	X		X	X	X	X			X	X
DES	X	X	X	X	X		X	X	X	X			X	X
DESede	X	X	X	X	X		X	X	X	X			X	X
DESedeWrap	X									X				
Rijndael	X	X	X	X	X	X	X	X	X	X			X	X
RSA				X							X	X		
Serpent	X	X	X	X	X		X	X	X	X			X	X
Twofish	X	X	X	X	X		X	X	X	X			X	X

The Blowfish, CAST, Serpent, and Twofish algorithms are not supported for modules with firmware version 2.33.60 or later.

Algorithm	Key length in bits for generation or signing	Use for ...									
		KeyGenerator	KeyPairGenerator	Signature	Cipher	KeyAgreement	KeyFactory	KeyStore	MAC	MessageDigest	SecureRandom
AESWrap					Y						
Arcfour	8, 16 to 2048	Y			Y						
Blowfish	32, 40 to 448	Y			Y						
CAST	40, 48 to 128	Y			Y						
CAST256	128, 192, 256	Y			Y						
DES	64	Y			Y						
DESede	192	Y			Y						
DES2	128	Y			Y						

Algorithm	Key length in bits for generation or signing	Use for ...									
		KeyGenerator	KeyPairGenerator	Signature	Cipher	KeyAgreement	KeyFactory	KeyStore	MAC	MessageDigest	SecureRandom
DESedeWrap					Y						
DH			Y			Y	Y				
DSA	1024		Y				Y				
ECDH			Y			Y	Y				
ECDSA			Y				Y				
HmacMD5		Y							Y		
HmacRIPEMD160	8, 16 to 2048	Y							Y		
HmacSHA1	8, 16 to 2048	Y							Y		
HmacSHA224	8, 16 to 2048	Y							Y		
HmacSHA256	8, 16 to 2048	Y							Y		
HmacSHA384	8, 16 to 2048	Y							Y		
HmacSHA512	8, 16 to 2048	Y							Y		
HmacTiger	8, 16 to 2048	Y							Y		
MD5										Y	
MD5andSHA1withRSA				Y							
MD5withRSA				Y							
nCipher.sworld								Y			
Rijndael		Y			Y						
RawRSA				Y							
RIPEMD160withRSA				Y							
RIPEMD160withRSAandMGF1	322+			Y							
RND											Y
RSA	512+		Y		Y		Y				
Serpent	8, 16 to 256	Y			Y						
SHA1										Y	
SHA1withDSA				Y							

Algorithm	Key length in bits for generation or signing	Use for ...									
		KeyGenerator	KeyPairGenerator	Signature	Cipher	KeyAgreement	KeyFactory	KeyStore	MAC	MessageDigest	SecureRandom
SHA1withECDSA				Y							
SHA1withRSA				Y							
SHA1withRSAandMGF1	322+			Y							
SHA224										Y	
SHA224withDSA				Y							
SHA224withECDSA				Y							
SHA224withRSA				Y							
SHA224withRSAandMGF1	450+			Y							
SHA256										Y	
SHA256withDSA				Y							
SHA256withECDSA				Y							
SHA256withRSA				Y							
SHA256withRSAandMGF1	514+			Y							
SHA384										Y	
SHA384withDSA				Y							
SHA384withECDSA				Y							
SHA384withRSA				Y							
SHA384withRSAandMGF1	770+			Y							
SHA512										Y	
SHA512withDSA				Y							
SHA512withECDSA				Y							
SHA512withRSA				Y							
SHA512withRSAand MGF1	1026+			Y							
Tiger	8, 16 to 256	Y			Y						

The Blowfish, CAST, Serpent, Twofish, and MD5withRSA algorithms are not supported for modules with firmware version 2.33.60 or later.

7.6 The KeyStore API

You can load and store nShield module-protected keys by using the standard KeyStore API. This interface allows access to a KeyStore data file by means of a pass phrase and an **`InputStream`** or **`OutputStream`**.

nShield KeyStore data files contain only the name-space identifier of the keys stored in them; the actual keys are stored in the Security World regardless of the stream used. The name-space identifier is the hash of the root key of the individual KeyStore. The **`ident`** of the KeyStore keys in the Security World begins with this hash and is followed by key-specific characters. This naming hierarchy allows you to identify the relevant key in Security World tools (such as KeySafe) and remove keys from a KeyStore.

To use an existing KeyStore on another machine in the same Security World, copy both its KeyStore data file and the Security World's Key Management Data directory to the other machine.

7.7 Initialization

You create a new KeyStore by passing a null **`InputStream`** to the KeyStore load method. When you create a new KeyStore, the nCipherKM provider generates a KeyStore key that is used to sign trusted public certificate entries. The relevant signature is verified when public certificates in the KeyStore are used; this functionality prevents an attacker inserting new certificates into a KeyStore without the protection token that is needed to use the KeyStore key.

By default, the KeyStore protection key is OCS-protected. Ensure that the pass phrase argument used with the KeyStore interface matches the pass phrase of that OCS. When the KeyStore method is called, you must present a card with a matching pass phrase from the required OCS. You can use the **`protect`** system property to change the protection type used for the KeyStore key; for more information about the **`protect`** property, see *System properties* on page 95.

An existing KeyStore file is not overwritten if the KeyStore store method is called on an **`OutputStream`** directed at the same file path. Instead, the KeyStore at the existing path is used to store the keys in the new KeyStore. This operation fails if the pass phrases for the two KeyStores do not match.

7.8 Loading and storing keys

We recommend that separate KeyStores are used for separate purposes; for example, you can use one KeyStore to hold private keys and a different KeyStore for Certifying Authorities. With this approach, you need separate OCSs to operate separate KeyStores. However, you can also use different OCSs to protect keys within the same KeyStore.

You require a certificate chain to store private keys. The Virtual Machine JCE implementation enforces this requirement, not the nCipherKM provider.

7.9 keytool

You can use either the Oracle **keytool** utility or the IBM **keytool** utility to read and edit an nShield KeyStore. These utilities are shipped with the Oracle and IBM JVMs. You must specify the correct **nCipher.sworld** KeyStore type when you run the **keytool** utility, and you must specify the correct package name for the Oracle or IBM **keytool** utility.

To generate a new key in an OCS-protected KeyStore with the Oracle or IBM **keytool** utility, run the appropriate command:

- Sun Microsystems **keytool** utility:

  For Java 8, use the following command:

  ```
  java sun.security.tools.keytool.Main -genkey -storetype nCipher.sworld -keyalg RSA -sigalg
  SHA1withRSA -storepass KeyStore_passphrase -keystore KeyStore_path
  ```

  For Java 7 or earlier, use the following command:

  ```
  java sun.security.tools.KeyTool -genkey -storetype nCipher.sworld -keyalg RSA -sigalg
  SHA1withRSA -storepass KeyStore_passphrase -keystore KeyStore_path
  ```

- IBM **keytool** utility:

  ```
  java com.ibm.crypto.tools.KeyTool -genkey -storetype nCipher.sworld -keyalg RSA -sigalg
  SHA1withRSA -storepass KeyStore_passphrase -keystore KeyStore_path
  ```

In these example commands, *KeyStore_passphrase* is the pass phrase for the OCS that protects the KeyStore and *KeyStore_path* is the path to that KeyStore.

To generate a new key in a module-protected KeyStore with the Oracle or IBM **keytool** utility, run the appropriate command:

- Sun Microsystems **keytool** utility:

  For Java 8, use the following command:

  ```
  java -Dprotect=module -DignorePassphrase=true sun.security.tools.keytool.Main -genkey -
  storetype nCipher.sworld -keyalg RSA -sigalg SHA1withRSA -keystore KeyStore_path
  ```

  For Java 7 or earlier, use the following command:

  ```
  java -Dprotect=module -DignorePassphrase=true sun.security.tools.KeyTool -genkey -
  storetype nCipher.sworld -keyalg RSA -sigalg SHA1withRSA -keystore KeyStore_path
  ```

- IBM **`keytool`** utility:

```
java -Dprotect=module -DignorePassphrase=true com.ibm.crypto.tools.KeyTool -genkey -
storetype nCipher.sworld -keyalg RSA -sigalg SHA1withRSA -keystore KeyStore_path
```

In these example commands, *KeyStore_path* is the path to the KeyStore.

By default, the **`keytool`** utilities use the **`MD5withRSA`** signature algorithm to sign certificates used with a KeyStore. This signature mechanism is unavailable on modules with firmware version 2.33.60 or later.

7.10 Using keys

Only the nCipherKM provider can use keys stored in an nShield KeyStore because the underlying key material is held separately in the Security World.

You can always store nShield keys in an nShield KeyStore. You can also store keys generated by a third-party provider into an nShield KeyStore if both of the following conditions apply:

- the key type is known to the nCipherKM provider
- the Security World is *not* compliant with FIPS 140-2 level 3.

When you generate an nShield key (or create it from imported key material), that key is associated with an ACL (Access Control List). This ACL prevents the key from being used for operations for which it is unsuited and enforces requirements that certain tokens be presented; for example, the ACL can specify that signing key cannot be used for encryption.

Appendix A Glossary

Authorized Card List

Controls the use of Remote Administration cards. If the serial number of a card does not appear in the Authorized Card List, it is not recognized by the system and cannot be used. The list only applies to Remote Administration cards.

Access Control List (ACL)

An Access Control List is a set of information contained within a key that specifies what operations can be performed with the associated key object and what authorization is required to perform each of those operations.

Administrator Card Set (ACS)

Part of the Security World architecture, an Administrator Card Set (ACS) is a set of smart cards used to control access to Security World configuration, as well as recovery and replacement operations.

The Administrator Cards containing share in the logical tokens that protect the Security World keys, including K_{NSO}, the key-recovery key, and the recovery authorization keys. Each card contains one share from each token. The ACS is created using the well-known module key so that it can be loaded onto any nShield module.

See also *Security World*, *Operator Card Set (OCS)*

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a block cipher adopted as an encryption standard by the US government and officially documented as US FIPS PUB 197 (FIPS 197). Originally only used for non-classified data, AES was also approved for use with for classified data in June 2003. Like its predecessor, the Data Encryption Standard (DES), AES has been analyzed extensively and is now widely used around the world.

Although AES is often referred to as *Rijndael* (the cipher having been submitted to the AES selection process under that name by its developers, Joan Daemen and Vincent Rijmen), these are not precisely the same cipher. Technically, Rijndael supports a larger range of block and key sizes (at any multiple of 32 bits, to a minimum of 128 bits and a maximum of 256 bits); AES has a fixed block size of 128 bits and only supports key sizes of 128, 192, or 256 bits.

See also *Data Encryption Standard (DES)* on page 107

Audit logging

Audit logging, also known as syslog-sign, adds a number of control messages to the log entries that are to be audited:

- Logs generated and signed on HSM
- Tamper detection
- Deletion Detection
- Optional key usage logging
- Public key verification of audit logs
- Compatibility with syslog and SIEM.

CAST

CAST is a symmetric encryption algorithm with a 64-bit block size and a key size of between 40 bits to 128 bits (but only in 8-bit increments).

client identifier: R_{SC}

This notation represents an arbitrary number used to identify a client. In the nCore API, all client identifiers are 20 bytes long.

Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric cipher approved by NIST for use with US Government messages that are Secure but not Classified. The implementation of DES used in the module has been validated by NIST. DES uses a 64-bit block and a 56-bit key. DES keys are padded to 64 bits with 8 parity bits.

See also *Triple DES* on page 112, *Advanced Encryption Standard (AES)* on page 106

Diffie-Hellman

The Diffie-Hellman algorithm was the first commercially published public key algorithm. The Diffie-Hellman algorithm can only be used for key exchange.

Digital Signature Algorithm (DSA)

Also known as the Digital Signature Standard (DSS), the Digital Signature Algorithm (DSA) is a digital signature mechanism approved by NIST for use with US Government messages that are Secure but not Classified. The implementation of the DSA used by nShield modules has been validated by NIST as complying with FIPS 186.

Digital Signature Standard (DSS)

See *Digital Signature Algorithm (DSA)* on page 107

ECDH

A variant of the Diffie-Hellman anonymous key agreement protocol which uses elliptic curve cryptography.

See also *Diffie-Hellman* on page 107.

ECDSA

Elliptic Curve DSA: a variant of the Digital Signature Algorithm (DSA) which uses elliptic curve cryptography.

See also *Digital Signature Algorithm (DSA)* on page 107, *Diffie-Hellman* on page 107.

encryption: $\{A\}_B$

This notation indicates the result of **A** encrypted with key **B**.

Federal Information Processing Standards (FIPS)

The Federal Information Processing Standards (FIPS) were developed by the United States federal government for use by non-military government agencies and government contractors. FIPS 140 is a series of publications intended to coordinate the requirements and standards for cryptographic security modules, including both their hardware and software components.

All Security Worlds are compliant with FIPS 140-2. By default, Security Worlds are created to comply with FIPS 140-2 at level 2, but those customers who have a regulatory requirement for compliance with FIPS 140-2 at level 3 can also choose to create a Security World that meets those requirements.

For more details about FIPS 140-2, see http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

Hardserver

The hardserver software controls communication between applications and nShield modules, which may be installed locally or remotely. It runs as a service on the host computer. The behavior of the hardserver is controlled by the settings in the hardserver configuration file.

The hardserver software controls communication between the internal hardware security module and applications on the network. The module hardserver is configured using the front panel on the module or by means of uploaded configuration data. Configuration data is stored on the module and in files in a specially configured file system on each client computer.

hardware security module (HSM)

A hardware security module (commonly referred to as an HSM) is a hardware device used to hold cryptographic keys and software securely.

Hash: H(X)

This notation indicates a fixed length result that can be obtained from a variable length input and that can be used to identify the input without revealing any other information about it. The nShield module uses the Secure Hash Algorithm (SHA-1) for its internal security.

Identifier hash: $H_{ID}(X)$

An identifier hash is a hash that uniquely identifies a given object (for example, a key) without revealing the data within that object. The module calculates the identity hash of an object by hashing together the object type and the key material. The identity hash has the following properties:

$\mathbf{H}_{ID}$ is not modified by any operations on the key (for example, altering the ACL, the application data field, or other modes and flags)

H_{ID} is the same for both public and private halves of a key pair.

Unique data is added to the hash so that a H_{ID} is most unlikely to be the same as any other hash value that might be derived from the key material.

Key blob

A key blob is a key object with its ACL and application data encrypted by a module key, a logical token, or a recovery key. Key blobs are used for the long-term storage of keys. Blobs are cryptographically secure; they can be stored on the host computer's hard disk and are only readable by units that have access to the same module key.

See also *Access Control List (ACL)*.

Key object: K_A

This is a key object to be kept securely by the module. A key object may be a private key, a public counterpart to a private key, a key for a symmetric cipher (MAC or some other symmetric algorithm), or an arbitrary block of data. Applications can use this last type to allow the module to protect any other data items in the same way that it protects cryptographic keys. Each key object is stored with an ACL and a 20-byte data block that the application can use to hold any relevant information.

KeyID: ID_{KA}

When a key object KA is loaded within the module's RAM, it is given a short identifier or handle that is notated as ID_{KA}. This is a transient identifier, not to be confused with the key hash **HID(KA)**.

Logical token: K_T

A logical token is a key used to protect key blobs. A logical token is generated on the nShield module and never revealed, except as shares.

MAC: MAC_{KC}

This notation indicates a MAC (Message Authentication Code) created using key **KC**.

Module

See *hardware security module (HSM)*.

Module key: K_M

A module key is a cryptographic key generated by each nShield module at the time of initialization and stored within the module. It is used to wrap key blobs and key fragments for tokens. Module keys can be shared across several modules to create a larger Security World.

All modules include two module keys:

- module key zero K_{M0}, a module key generated when the module is initialized and never revealed outside the module.
- **null**, or well-known module key K_{MWK}.

You can program extra module keys into a module.

See also: *Security World*, *hardware security module (HSM)*.

Module signing key: K_{ML}

The module signing key is the module’s public key. It is used to issue certificates signed by the module. Each module generates its own unique K_{ML} and K_{ML}^{-1} values when it is initialized. The private half of this key pair, K_{ML}^{-1}, is never revealed outside the module.

nShield master feature enable key K_{SA}

Certain features of the module firmware are available as options. These features must be purchased separately from nCipher. To use a feature on a specific module, you require a certificate from nCipher signed by K_{SA}. These certificates include the electronic serial number for the module.

nShield Remote Administration Card

Smart cards that are capable of negotiating cryptographically secure connections with an HSM, using warrants as the root of trust. nShield Remote Administration Cards can also be used in the local slot of an HSM if required. You must use nShield Remote Administration Cards with Remote Administration.

nShield Security Officer's key: K_{NSO}^{-1}

The notation K_{NSO}^{-1} indicates the Security Officer’s signing key. This key is usually a key to a public-key signature algorithm.

nShield Trusted Verification Device

A smart card reader that allows the card holder to securely confirm the Electronic Serial Number (ESN) of the HSM to which they want to connect, using the display of the device. nCipher supplies and the nShield Trusted Verification Device and recommends its use with Remote Administration.

Null module key: K_{MWK}

The null module key is used to create tokens that can be loaded onto any module. Such tokens are required for recovery schemes. The null module key is a Triple DES key of a value 01010101. As this value is well known, this module key does not have any security. Key blobs cannot be made directly under the null module key. To make a blob under a token protected by the null module key, the key must have the ACL entry **AllowNullKMToken**.

Operator Card Set (OCS)

Part of the Security World architecture, an Operator Card Set (OCS) is a set of smart cards containing shares of the logical tokens that is used to control access to application keys within a Security World. OCSs are protected using the Security World key, and therefore they cannot be used outside the Security World.

See also: *Security World*, *Administrator Card Set (ACS)*.

Recovery key: K_{RA}

The recovery key is the public key of the key recovery agent.

Remote access solution

The remote access solution, such as SSH or a remote desktop application, which is used as standard by your organization. Enables you to to carry out Security World administrative tasks from a different location to that of an nShield Connect or nShield Solo.

For example, the remote access solution is used to run Security World utilities remotely and to enter passphrases.

nCipher does not provide this software.

Remote Administration

An optional Security World feature that enables Remote Administration card holders to present their cards to an HSM located elsewhere. For example, the card holder may be in an office, while the HSM is in a data center. Remote Administration supports the ACS, as well as persistent and non-persistent OCS cards, and allows all smart card operations to be carried out, apart from loading feature certificates.

nShield Remote Administration Client

A GUI or command-line interface that enables you to select an HSM located elsewhere from a list provided by the Remote Administration Service, and associate a card reader attached to your computer with the HSM. Resides on your local Windows or Linux-based computer.

Remote Administration Service

Enables secure communications between an nShield Remote Administration Card and the hardserver that is connected to the appropriate HSM. Listens for incoming connection requests from nShield Remote Administration Clients. Supplies a list of available HSMs to the nShield Remote Administration Client and maintains an association between the relevant card reader and the HSM.

Dynamic Slot

Virtual card slots that can be associated with a card reader connected to a remote computer. Remote Administration Slots are in addition to the local slot of an HSM and any soft card slot that may be available. HSMs have to be configured to support between zero (default) and 16 Remote Administration Slots.

Rijndael

See *Advanced Encryption Standard (AES)* on page 106

Salt: X

The random value, or salt, is used in some commands to discourage brute force searching for keys.

Security World

The Security World technology provides an infrastructure for secure lifecycle management of keys. A Security World consists of at least one HSM, some cryptographic key and certificate data encrypted by a Security World key and stored on at least one host computer, a set of Administrator Cards used to control access to Security World configuration, recovery and replacement operations, and optionally one or more sets of Operator Cards used to control access to application keys.

See also *Administrator Card Set (ACS)*, *Operator Card Set (OCS)*.

Security World key: K_{MSW}

The Security World key is the module key that is present on all modules in a Security World. Each Security World has a unique Security World key. This key is generated randomly when the Security World is created, and it is stored as a key blob protected by the ACS.

Share: K_{Ti}

The notation K_{Ti} indicates a share of a logical token. Shares can be stored on smart cards or software tokens. Each share is encrypted under a separate share key.

Share key: K_{Si}

A share key is a key used to protect an individual share in a token. Share keys are created from a Security World key, a pass phrase, and a salt value.

Standard nShield Cards

Smart cards used in the local slot of an HSM. Standard nShield cards are not supported for use with Remote Administration.

Standard card reader

A smart card reader for ISO/IEC 7816 compliant smart cards. nCipher recommends that standard smart card readers are only used with the nShield Remote Administration Client command-line utility, not the GUI.

Triple DES

Triple DES is a highly secure variant of the Data Encryption Standard (DES) algorithm in which the message is encrypted three times.

See also *Data Encryption Standard (DES)* on page 107, *Advanced Encryption Standard (AES)* on page 106.