



nShield Security World

nCipherKM JCA JCE CSP v13.4.5 API Guide

17 October 2024

Table of Contents

1. Introduction	1
1.1. Read this guide if.....	1
1.2. Model numbers	1
1.3. Security World Software default directories	2
1.4. Utility help options	4
1.5. Further information	4
1.6. Security advisories	4
1.7. Contacting Entrust nShield Support	5
2. nShield Architecture	6
2.1. Security World Software modules	6
2.2. Security World Software server	6
2.3. Stubs and interface libraries	7
2.4. Using an interface library	7
2.5. Writing a custom application	8
2.6. Acceleration-only or key management	8
3. Installing the nCipherKM JCA/JCE CSP	9
3.1. Prerequisites	9
3.2. Installing the nCipherKM JCA/JCE CSP	9
3.3. Testing the nCipherKM JCA/JCE CSP installation	12
3.4. Named Modules in Java 11 and Java 17	14
4. System Properties	16
4.1. JCECSP_DEBUG property values	17
5. Compatibility	19
6. Architecture	20
6.1. Architecture	20
7. Available Functions	22
7.1. Available functions	22
8. The KeyStore API	27
9. Initialization	28
10. Loading and Storing Keys	29
11. keytool	30
12. Using Keys	32

1. Introduction

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

This guide describes the nCipherKM JCA/JCE cryptographic service provider toolkit supplied by Entrust Security to help developers write applications that use nShield modules.

This toolkit, like the application plug-ins supplied by Entrust, uses 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 an nShield 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. Model numbers

Model numbering conventions are used to distinguish different nShield hardware security devices. In the following table, *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+

Model number	Used for
NH2054	nShield Connect 500+
NH2075-B	nShield Connect XC Base
NH2075-M	nShield Connect XC Medium
NH2075-H	nShield Connect XC High
NH2075-B	nShield 5c Base
NH2075-M	nShield 5c Medium
NH2075-H	nShield 5c High
NH2082	nShield Connect XC SCAP
NH2089-B	nShield Connect XC Base - Serial Console
NH2089-M	nShield Connect XC Mid - Serial Console
NH2089-H	nShield Connect XC High - Serial Console
NH3003-B	nShield Connect CLX Base - Serial Console
NH3003-M	nShield Connect CLX Mid - Serial Console
NH3003-H	nShield Connect CLX High - Serial Console
nC2021E-000, NCE2023E-000	nToken PCIe
nC3nnnE-nnn, nC4nnnE-nnn	nShield Solo PCIe
nC30n5E-nnn, nC40n5E-nnn	nShield Solo XC PCIe
nC30nnU-10, nC40nnU-10	nShield Edge
NC5536E-B	nShield 5s Base
NC5536E-M	nShield 5s Medium
NC5536E-H	nShield 5s High

1.3. Security World Software 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 2016	Linux
nShield Installation	NFAST_HOME	C:\Program Files\nCipher\nfast	/opt/nfast/

Directory Name	Environment Variable	Windows Server 2016	Linux
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/



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**.



Dynamic feature certificates must be stored in the directory stated in the default directories table.

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 in percent signs (for example, **%NFAST_KMDATA%**).
- For Linux, absolute paths (for example, **/opt/nfast/kmdata/**).

NFAST_KMDATA cannot be a symbolic link.

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 Linux, 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.

1.4. 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.

1.5. Further information

This guide forms one part of the information and support provided by Entrust.

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`
- Linux:
 - 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.

1.6. Security advisories

If Entrust becomes aware of a security issue affecting nShield HSMs, Entrust 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 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. Because of this, you should consider the procedures and actions required to upgrade devices in the field when deploying and maintaining your HSMs.



The Remote Administration feature supports remote firmware upgrade of nShield HSMs, and remote ACS card presentation.

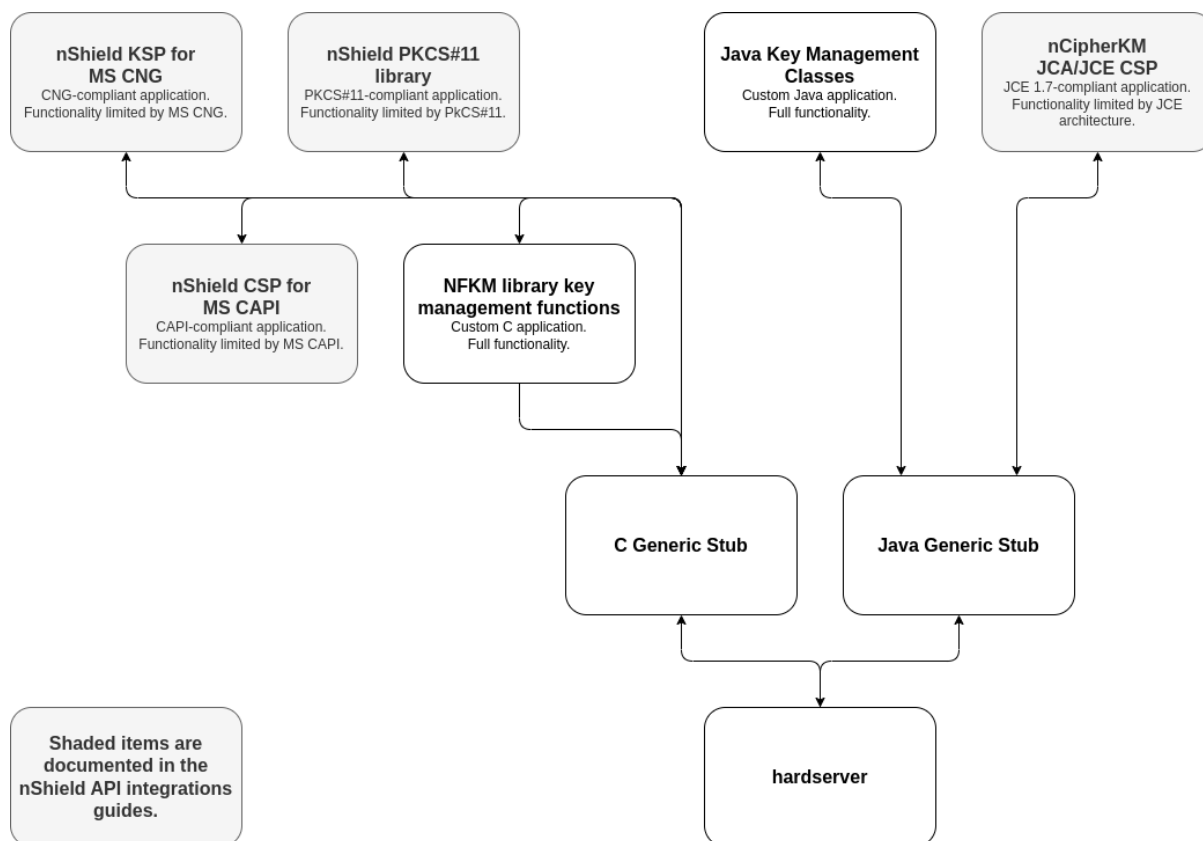
We recommend that you monitor the Announcements & Security Notices section on Entrust nShield, <https://nshieldsupport.entrust.com>, where any announcement of nShield Security Advisories will be made.

1.7. Contacting Entrust nShield Support

To obtain support for your product, contact Entrust nShield Support, <https://nshieldsupport.entrust.com>.

2. nShield Architecture

This chapter provides a brief overview of the Security World Software architecture. The following diagram provides a visual representation of nShield architecture and the documentation that relates to it.



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 domain socket on Linux 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 Entrust 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

Entrust supplies the following interface libraries:

- Microsoft Cryptography API: Next Generation (CNG)
- Microsoft CryptoAPI (CAPI)
- 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 Entrust 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, Entrust provides generic stub libraries for C and Java. If you want to use a language other than C or Java, you must write your own wrapper functions in your chosen programming language that call the C generic stub functions.

Entrust 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 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. Installing the nCipherKM JCA/JCE CSP

3.1. Prerequisites

To use the nCipherKM JCA/JCE CSP, you must install the nShield Java package which includes the nShield Java jars and Keysafe.

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 nShield Security World Software:

- Java 8 (or Java 1.8x)
- Java 11
- Java 17

We recommend 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 Entrust 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 nShield software, please contact Entrust nShield Support:

<https://nshieldsupport.entrust.com>.

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:

- <http://www.oracle.com/technetwork/java/index.html>
- <http://www.oracle.com/technetwork/java/all-142825.html>



Detailed documentation for the JCE interface can be found on the Oracle Technology web page [here](#).



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

3.2. 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, restart the hardserver before continuing the nCipherKM JCA/JCE CSP installation process. For more information, see the *User Guide* for your HSM.

2. For Java 8 only. Copy the `nCipherKM.jar` file to the extensions folder of your local Java Virtual Machine installation from the following directory:

- `%NFAST_HOME%\java\classes` (Windows)
- `/opt/nfast/java/classes` (Linux)

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

JVM type	Extensions folder (Windows)	Extensions folder (Linux)
Java Developer Kit (JDK)	<code>%JAVA_HOME%\jre\lib\ext</code>	<code>\$JAVA_HOME/jre/lib/ext</code>
Java Runtime Environment (JRE)	<code>%JAVA_HOME%\lib\ext</code>	<code>\$JAVA_HOME/_lib/ext</code>

In these paths, `%JAVA_HOME%` (Windows) and `$JAVA_HOME` (Linux) are the home directory of the Java installation (commonly specified in the `JAVA_HOME` environment variable).

If you are using Java 11 or Java 17 you do not need to copy the jar file.

3. Add `%JAVA_HOME%\bin` (Windows) or `$JAVA_HOME/bin` (Linux) to your `PATH` system variable.
4. For Java 8 only. Install the unlimited strength JCE jurisdiction policy files that are appropriate to your version of Java. JDK 9 and later ship with, and use by default, the unlimited policy files.

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.

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

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.



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 (Windows)	Extensions folder (Linux)
Java Developer Kit (JDK)	<code>%JAVA_HOME%\jre\lib\security</code>	<code>\$JAVA_HOME/jre/lib/security</code>
Java Runtime Environment (JRE)	<code>%JAVA_HOME%\lib\security</code>	<code>\$JAVA_HOME_/lib/security</code>

In these paths, `%JAVA_HOME%` (Windows) and `$JAVA_HOME` (Linux) are the home directory of the Java installation (commonly specified in the `JAVA_HOME` environment variable).



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` file located in the security directory for your local Java Virtual Machine (JVM) installation: `security.provider.<n>=com.ncipher.provider.km.nCipherKM`, where `<n>` is the position in the list of providers, for example:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=sun.security.rsa.SunRsaSign
security.provider.3=com.sun.net.ssl.internal.ssl.Provider
security.provider.4=com.sun.crypto.provider.SunJCE
```

```
security.provider.5=sun.security.jgss.SunProvider
security.provider.6=com.sun.security.sasl.Provider
security.provider.7=com.ncipher.provider.km.nCipherKM
```

For Java 11 and Java 17 you do not need to specify the fully qualified class name for the provider. Instead you can just use the provider name: `security.provider.<n>=nCipherKM`.

The JVM uses this file to select the provider from which to request a mechanism instance. If your JCE application does not request the nCipherKM provider by name, or if it fails to load keys, you might need to move the nCipherKM provider to the top of the list: `security.provider.1=com.ncipher.provider.km.nCipherKM`. Do not change the relative order of the other providers in the list.



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). If you add the nCipherKM provider as `security.provider.1`, ensure that the subsequent providers are re-numbered correctly.

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.

3.3. 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.

For Java 8:

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

For Java 11 and Java 17 (Windows):

```
java --module-path %NFAST_HOME%\java\classes com.ncipher.provider.InstallationTest
```

For Java 11 and Java 17 (Linux):

```
java --module-path /opt/nfast/java/classes com.ncipher.provider.InstallationTest
```



For these commands to work, you must have added `%JAVA_HOME%` (Windows) or `$JAVA_HOME` (Linux) 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](#).

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](#). 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](#).

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.



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](#).

3.4. Named Modules in Java 11 and Java 17

The nCipherKM Provider has been implemented as a named module. This means that, for Java 11 and Java 17, if you have added the provider to your **java.security** file, then you can run your application with the **nCipherKM.jar** on the module-path and the Java Service-Loader class will automatically find it, for example:

In Linux:

```
java --module-path /opt/nfast/java/classes com.ncipher.provider.InstallationTest
```

In Windows:


```
java --module-path %NFAST_HOME%\java\classes com.ncipher.provider.InstallationTest
```

Alternatively, you can specify the location of the nCipherKM jar on the classpath:

In Linux:

```
java --class-path /opt/nfast/java/classes/nCipherKM.jar com.ncipher.provider.InstallationTest
```

In Windows:

```
java --class-path %NFAST_HOME%\java\classes\nCipherKM.jar com.ncipher.provider.InstallationTest
```

4. 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 -D<property>=<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 .
JCECSP_DEBUGFILE	<p>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.</p> <p>In a production environment, we recommend that you disable debug logging to prevent sensitive information being made available to an attacker.</p>
CKNFAST_JCE_COMPATIBILITY	This property is included to allow the saving of objects when using Java PKCS#11 providers.
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.

Property	Function for different values
<code>ignorePassphrase</code>	If the value of this property is set to <code>true</code> , the nCipherKM provider ignores the passphrase provided in its KeyStore implementation. This feature is included to allow the Oracle or IBM <code>keytool</code> utilities to be used with module-protected keys. The <code>keytool</code> utilities require a passphrase be provided; setting this property allows a dummy passphrase to be used.
<code>seeintegname</code>	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.
<code>com.ncipher.provider.announce-mode</code>	The default value for this property is <code>auto</code> , 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 <code>on</code> forces the provider to advertise all mechanisms at start-up. Setting the value of this property to <code>off</code> forces the provider to advertise no mechanisms at start-up.
<code>com.ncipher.provider.enable</code>	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.
<code>com.ncipher.provider.disable</code>	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 <code>com.ncipher.provider.disable</code> property overrides the same mechanism if it is supplied in the value for the <code>com.ncipher.provider.enable</code> property.

4.1. 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, <code>debugFunc</code> and <code>debugFuncEnd</code> generate debugging information for functions that call them.

JCECSP_DEBUG value	Function
16	If this property has the bit 5 set, <code>debugFunc</code> and <code>debugFuncEnd</code> 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 <code>ThreadID</code> 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`.

5. 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 at either Level 2 or Level 3.



In a Security World that complies with FIPS 140 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 passphrase.

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 passphrase used with the KeyStore must be the passphrase of the card from the OCS that protects the keys in the KeyStore.

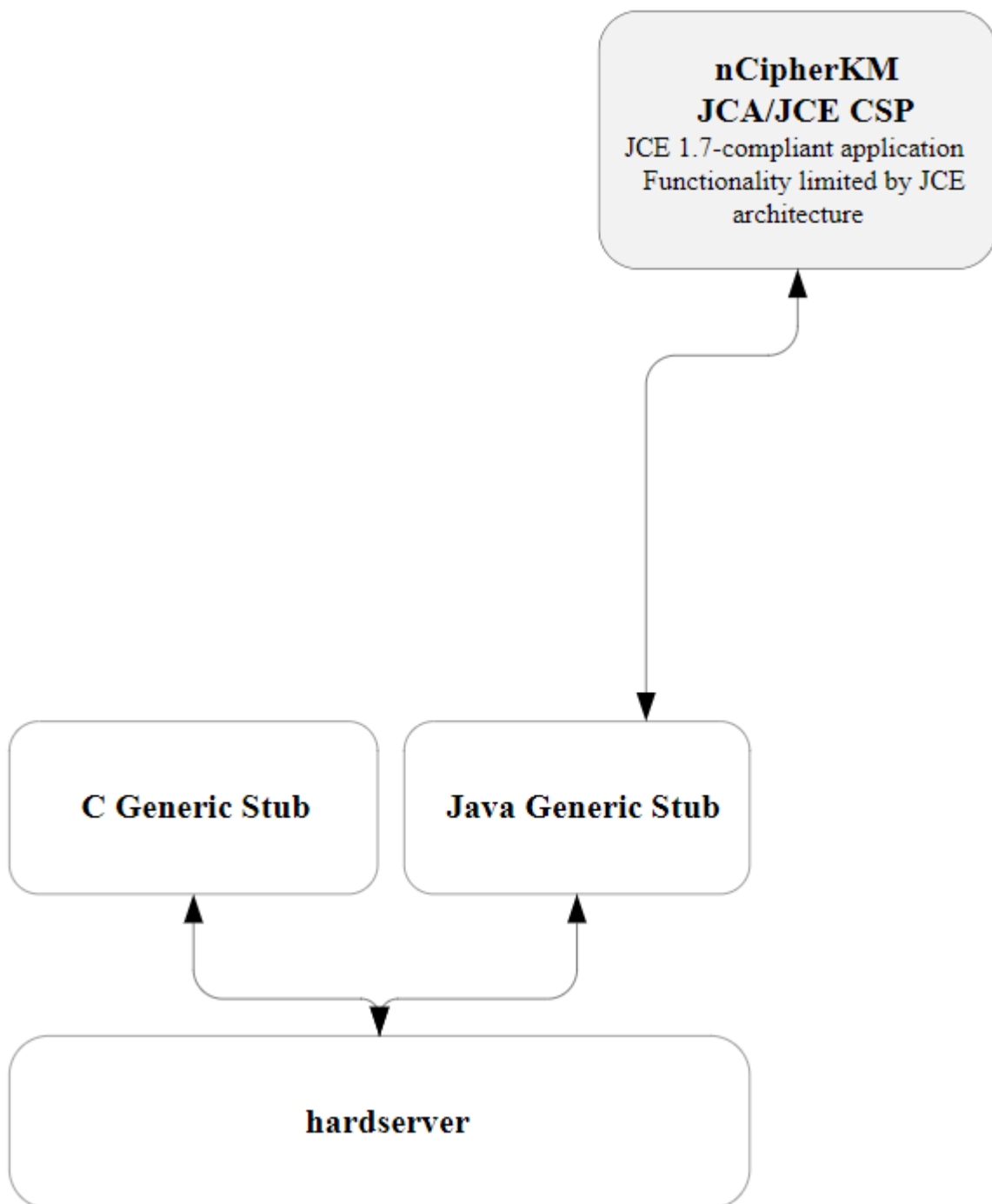
6. Architecture

6.1. 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 hardware and modules.



7. Available Functions

7.1. 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.

The following table indicates the cipher modes available for each cipher.

Cipher	CBC	CFB	CTR	ECB	OFB	GCM
AESWrap				X		
ArcFour						
CAST256	X	X	X	X	X	
DES2	X	X	X	X	X	
DES	X	X	X	X	X	
DESede	X	X	X	X	X	
DESedeWrap	X					
ECIES ¹						
Rijndael	X	X	X	X	X	X
RSA				X		

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

¹ These ciphers support key wrap and unwrap only.

The following table indicates the padding types available for each cipher.

Cipher	ANSI X9.23	ISO 10126	ISO 7816	None	OAEP	PKCS #1	PKCS #5	Zero byte
AESWrap				X				
ArcFour								
CAST256	X	X	X	X			X	X

Cipher	ANSI X9.23	ISO 10126	ISO 7816	None	OAEP	PKCS #1	PKCS #5	Zero byte
DES2	X	X	X	X			X	X
DES	X	X	X	X			X	X
DESede	X	X	X	X			X	X
DESedeWrap				X				
ECIES ¹								
Rijndael	X	X	X	X			X	X
RSA				X	X			

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

¹ These ciphers support key wrap and unwrap only.

Algorithm	Key length in bits for gener- ation or sign- ing	KeyGenerator	KeyPairGenerator	Signature	Cipher	KeyAgreement	KeyFactory	KeySafe	Mac	MessageDigest	SecureRandom
AESWrap					Y						
Arcfour	8, 16 to 2048	Y ¹			Y ¹						
CAST256	128, 192, 256	Y ¹			Y ¹						
DES	64	Y ¹			Y ¹						
DESede	192	Y			Y						
DES2	128	Y			Y						
DESedeWrap					Y						
DH			Y			Y	Y				
DSA	1024		Y				Y				
ECDH			Y			Y	Y				
ECD- HwithSHA1KD F						Y					

Algorithm	Key length in bits for generation or signing	KeyGenerator	KeyPairGenerator	Signature	Cipher	KeyAgreement	KeyFactory	KeySafe	Mac	MessageDigest	SecureRandom
ECD-HwithSHA224 KDF						Y					
ECD-HwithSHA256 KDF						Y					
ECD-HwithSHA384 KDF						Y					
ECD-HwithSHA512 KDF						Y					
ECDSA			Y				Y				
EdDSA	256		Y ¹				Y ¹				
Ed25519	256		Y ¹	Y ¹							
Ed25519ph				Y ¹							
HmacMD5		Y ¹							Y ¹		
HmacRIPEMD 160	8, 16 to 2048	Y ¹							Y ¹		
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 ¹							Y ¹		
MD5										Y ¹	
MD5and-SHA1withRSA				Y							
MD5withRSA				Y							

Algorithm	Key length in bits for generation or signing	KeyGenerator	KeyPairGenerator	Signature	Cipher	KeyAgreement	KeyFactory	KeySafe	Mac	MessageDigest	SecureRandom
nCipher.ssworld								Y			
Rijndael		Y			Y						
RawRSA				Y							
RIPEMD160										Y ¹	
RIPEMD160withRSA				Y ¹							
RIPEMD160withRSAandMGF1	322+			Y ¹							
RNG											Y
RSA	512+		Y		Y		Y				
SHA1										Y	
SHA1withDSA				Y							
SHA1withECDSA				Y							
SHA1withRSA				Y							
SHA1withRSAandMGF1	322+			Y							
SHA224										Y	
SHA224withDSA				Y							
SHA224withECDSA				Y							
SHA224withRSA				Y							
SHA224withRSAandMGF1	450+			Y							
SHA256										Y	

Algorithm	Key length in bits for generation or signing	KeyGenerator	KeyPairGenerator	Signature	Cipher	KeyAgreement	KeyFactory	KeySafe	Mac	MessageDigest	SecureRandom
SHA256with-DSA				Y							
SHA256with-ECDSA				Y							
SHA256withRSA				Y							
SHA256withRSAandMGF1	514+			Y							
SHA384										Y	
SHA384with-DSA				Y							
SHA384with-ECDSA				Y							
SHA384withRSA				Y							
SHA384withRSAandMGF1	770+			Y							
SHA512										Y	
SHA512with-DSA				Y							
SHA512with-ECDSA				Y							
SHA512withRSA				Y							
SHA512withRSAandMGF1	1026+			Y							
Tiger	8, 16 to 256	Y			Y					Y ¹	

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

¹ These algorithms are not supported in FIPS 140 Level 3 Security Worlds.

8. 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 passphrase 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.

9. 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 passphrase argument used with the KeyStore interface matches the passphrase of that OCS. When the KeyStore method is called, you must present a card with a matching passphrase 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](#).

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 passphrases for the two KeyStores do not match.

10. 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.

11. 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.sworl**d 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 11 and Java 17, use the following command:

```
java --module-path /opt/nfast/java/classes sun.security.tools.keytool.Main -genkey -storetype nCipher.sworl -keyalg RSA -sigalg SHA1withRSA -storepass <KeyStore_passphrase> -keystore <KeyStore_path>
```

For Java 8, use the following command:

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

- IBM **keytool** utility:

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

In these example commands, **<KeyStore_passphrase>** is the passphrase 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 11 and Java 17, use the following command:

```
java --module-path /opt/nfast/java/classes -Dprotect=module -DignorePassphrase=true sun.security.tools.keytool.Main -genkey -storetype nCipher.sworl -keyalg RSA -sigalg SHA1withRSA -keystore <KeyStore_path>
```

For Java 8, use the following command:

```
java -Dprotect=module -DignorePassphrase=true sun.security.tools.KeyTool -genkey -storetype nCipher.sworl -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.

12. 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 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.