

# Security Policy

nShield F3 4000, nShield F3 2000, nShield F3 2000 for NetHSM,  
nShield F3 500, nShield F3 500 for NetHSM  
in FIPS 140-2 level 2 mode



**Version: 3.4**

**Date: 12 November 2015**

**Note:** Security Policy Certificate dates from Thales ownership. Some occurrences of "Thales" may still appear in text and images. These should be read as "nCipher".

Copyright © 2019 nCipher Security Limited. All rights reserved.

Copyright in this document is the property of nCipher Security Limited. It is not to be reproduced, modified, adapted, published, translated in any material form (including storage in any medium by electronic means whether or not transiently or incidentally) in whole or in part nor disclosed to any third party without the prior written permission of nCipher Security Limited neither shall it be used otherwise than for the purpose for which it is supplied.

Words and logos marked with ® or ™ are trademarks of nCipher Security Limited or its affiliates in the EU and other countries.

Information in this document is subject to change without notice.

nCipher Security Limited makes no warranty of any kind with regard to this information, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. nCipher Security Limited shall not be liable for errors contained herein or for incidental or consequential damages concerned with the furnishing, performance or use of this material.

Where translations have been made in this document English is the canonical language.

nCipher Security Limited  
Registered Office: One Station Square,  
Cambridge, CB1 2GA, United Kingdom  
Registered in England No. 11673268



## Versions

To support the range of nShield hardware platforms, multiple variants of this document are generated from the same source files.

| Version | Date              | Comments  |
|---------|-------------------|---|
| N/A     | 13 August 1998    | nFast nF75KM and nF75CA SCSI modules f/w 1.33.1   |
| N/A     | 18 January 2000   | nForce and nShield SCSI and PCI modules f/w 1.54.28   |
| N/A     | 20 December 2000  | nForce and nShield SCSI and PCI modules f/w 1.70  |
| N/A     | 1 March 2000      | nForce and nShield SCSI and PCI modules f/w 1.70  |
| 1.0.7   | 23 May 2001       | nForce and nShield SCSI and PCI modules f/w 1.71<br>Adds SEE  |
| 1.0.9   | 14 September 2001 | nForce and nShield SCSI and PCI modules f/w 1.71.91<br>Adds Remote Operator Card Sets, Foreign Token Access, Feature Enablement |
| 1.1.25  | 6 May 2002        | nForce and nShield SCSI and PCI modules f/w 1.77.96   |
| 1.1.30  | 22 July 2002      | nForce and nShield SCSI and PCI modules f/w 2.0.0   |
| 1.1.33  | 4 October 2002    | nForce and nShield SCSI and PCI modules f/w 2.1.12  |
| 1.2.39  | 23 June 2003      | nCipher PMC module f/w 2.1.32   |
| 1.3.3   | 3 July 2003       | nForce and nShield PCI 800 modules f/w 2.0.1  |
| 1.3.6   | 5 September 2003  | nForce and nShield SCSI and PCI modules f/w 2.0.2   |
| 1.0.24  | 23 January 2004   | nForce and nShield SCSI f/w 2.0.5   |
| 1.3.14  | 18 March 2004     | nForce, nShield and Payshield SCSI and PCI modules f/w 2.12<br>adds nCipher 1600 PCI  |
| 1.4.20  | 5 October 2005    | nForce, nShield and Payshield SCSI and PCI modules f/w 2,18   |
| 2.0.0   | 6 April 2006      | nShield 500 PCI f/w 2.22.6  |
| 1.4.14  | 9 March 2006      | nForce and nShield SCSI f/w 1.77.100 and PCI modules f/w 2.12.9 and 2.18.15<br>Fix for security issues                          |
| 1.4.28  | 15 March 2006     | nForce and nShield SCSI f/w 1.77.100 and PCI modules f/w 2.12.9 and 2.18.15<br>Typographic corrections to above.                |
| 2.0.1   | 11 May 2006       | nShield 500, 2000 and 4000 PCI f/w 2.22.6<br>MiniHSM f/w 2.22.6   |
| 2.1.1   | 14 June 2006      | nShield 500, 2000 and 4000 PCI f/w 2.22.34  |
| 2.1.2   | 29 August 2006    | MiniHSM build standard B  |
| 2.1.3   | 20 December 2006  | nShield 500 PCI f/w 2.22.34   |
| 2.2.2   | 29 April 2008     | nShield 500, 2000 and 4000 PCI f/w 2.2.43   |
| 2.2.3   | 24 June 2008      | nShield 500 PCI and nShield 500, 2000 and 4000 PCI f/w 2.33.60  |
| 2.3.1   | 15 December 2008  | nShield PCI and nShield PCIe f/w 2.33,75  |
| 2.4.1   | 28 August 2009    | nShield PCI and nShield PCIe f/w 2.33.82  |

| <b>Version</b> | <b>Date</b>       | <b>Comments</b>   |
|----------------|-------------------|---|
| 2.4.2          | 10 June 2009      | nShield PCI and nShield PCIe f/w 2.38.4                                       |
| 2.5.3          | 28 January 2010   | nShield PCI and nShield PCIe f/w 2.33.82                                      |
| 2.5.4          | 17 February 2010  | nShield PCI and nShield PCIe f/w 2.38.7                                       |
| 3.0            | 27 March 2012     | nShield PCI and nShield PCIe f/w 2.50.17 - Thales branding                    |
| 3.1            | 5 March 2013      | nShield PCI and nShield PCIe f/w 2.51.10                                      |
| 3.2            | 11 June 2013      | nShield PCI and nShield PCIe f/w 2.51.10, updated RSA certificates            |
| 3.3            | 15 September 2015 | nShield PCI and nShield PCIe f/w 2.50.16, 2.51.10, 2.50.35 and 2.55.1         |
| 3.4            | 12 November 2015  | nShield PCI and nShield PCIe f/w 2.50.16-3, 2.51.10-3, 2.50.35-3 and 2.55.1-3 |



# Contents

|  |           |
|--|-----------|
| <b>Chapter 1: Purpose</b>                          | <b>8</b>  |
| <b>Chapter 2: Module Ports and Interfaces</b>      | <b>12</b> |
| <b>Chapter 3: Excluded Components</b>              | <b>13</b> |
| <b>Chapter 4: Environmental Failure Protection</b> | <b>14</b> |
| <b>Chapter 5: Roles</b>                            | <b>15</b> |
| Unauthenticated                                    | 15        |
| User   | 15        |
| nCipher Security Officer                           | 15        |
| Junior Security Officer                            | 16        |
| <b>Chapter 6: Services available to each role</b>  | <b>17</b> |
| <b>Chapter 7: Keys</b>                             | <b>30</b> |
| nCipher Security Officer's key                     | 30        |
| Junior Security Officer's key                      | 30        |
| Long term signing key                              | 31        |
| Module signing key                                 | 31        |
| Module keys  | 31        |
| Logical tokens                                     | 32        |
| Share Key  | 32        |
| Impath keys  | 33        |
| Key objects  | 33        |
| Session keys                                       | 34        |
| Archiving keys                                     | 34        |
| Certificate signing keys                           | 35        |
| Firmware Integrity Key                             | 35        |
| Firmware Confidentiality Key                       | 36        |
| Master Feature Enable Key                          | 36        |
| DRBG Key   | 36        |

|   |           |
|---|-----------|
| <b>Chapter 8: Rules</b>   | <b>37</b> |
| Identification and authentication                                   | 37        |
| Access Control  | 37        |
| Access Control List   | 38        |
| Object re-use   | 39        |
| Error conditions  | 39        |
| Security Boundary   | 39        |
| Status information  | 39        |
|   | 40        |
| Procedures to initialise a module to comply with FIPS 140-2 Level 2 | 40        |
| Verifying the module is in level 2 mode                             | 40        |
| Operating a level 2 module in FIPS mode                             | 41        |
| To return a module to factory state                                 | 42        |
| To create a new operator  | 43        |
| To authorize the operator to create keys                            | 44        |
| To authorize an operator to act as a Junior Security Officer        | 45        |
| To authenticate an operator to use a stored key                     | 46        |
| To authenticate an operator to create a new key                     | 47        |
| <br>  |           |
| <b>Chapter 9: Physical security</b>                                 | <b>48</b> |
| Checking the module   | 48        |
| <br>  |           |
| <b>Chapter 10: Strength of functions</b>                            | <b>49</b> |
| Attacking Object IDs  | 49        |
| Attacking Tokens  | 49        |
| Key Blobs   | 50        |
| Impaths   | 50        |
| KDP key provisioning  | 51        |
| Derived Keys  | 51        |
| <br>  |           |
| <b>Chapter 11: Self Tests</b>                                       | <b>53</b> |
| Firmware Load Test  | 54        |

|   |           |
|---|-----------|
| <b>Chapter 12: Supported Algorithms</b> | <b>55</b> |
| FIPS approved and allowed algorithms:   | 55        |
| Symmetric Encryption                    | 55        |
| Hashing and Message Authentication      | 55        |
| Signature                               | 56        |
| Key Establishment                       | 56        |
| Other                                   | 57        |
| Non-FIPS approved algorithms            | 58        |
| Symmetric                               | 58        |
| Asymmetric                              | 58        |
| Hashing and Message Authentication      | 58        |
| Non-deterministic entropy source        | 59        |
| Other                                   | 59        |
| <b>Addresses</b>                        | <b>60</b> |
|   | <b>60</b> |

# Chapter 1: Purpose

nShield tamper resistant Hardware Security Modules are multi-tasking hardware modules that are optimized for performing modular arithmetic on very large integers. The modules also offer a complete set of key management protocols.

The nShield Hardware Security Modules are defined as multi-chip embedded cryptographic modules as defined by FIPS PUB 140-2.

| Unit ID                    | Model Number | RTC NVRAM | SEE      | Potting | EMC | Crypto Accelerator | Overall level |
|----------------------------|--------------|-----------|----------|---------|-----|--------------------|---------------|
| nShield F3 4000            | nC4033P-4KO  | Yes       | Optional | Yes     | B   | Broadcom 5821      | 2             |
| nShield F3 2000            | nC4033P-2KO  | Yes       | Optional | Yes     | B   | Broadcom 5821      | 2             |
| nShield F3 500             | nC4033P-500  | Yes       | Optional | Yes     | B   | Broadcom 5821      | 2             |
| nShield F3 2000 for NetHSM | nC4033P-2KON | Yes       | Optional | Yes     | B   | Broadcom 5821      | 2             |
| nShield F3 500 for NetHSM  | nC4033P-500N | Yes       | Optional | Yes     | B   | Broadcom 5821      | 2             |

The units are identical in operation and only vary in the processing speed and the support software supplied.

All modules are now supplied at build standard “N” to indicate that they meet the latest EU regulations regarding ROHS.

The nShield F3 2000 is fitted inside the NetHSM 2000 and provides all the security functions for this appliance.

The nShield F3 500 is fitted inside the NetHSM 500.



The NetHSM is shown below.



The following figure shows the module mounted inside the NetHSM



Thales also supply modules to third party OEM vendors for use in a range of security products.

The module runs firmware provided by Thales. There is the facility for the administrator to upgrade this firmware. In order to determine that the module is running the correct version of firmware they should use the **NewEnquiry** service which reports the version of firmware currently loaded.

The validated firmware versions are 2.50.16-3, 2.51.10-3, 2.50.35-3 and 2.55.1-3.

The initialization parameters are reported by the **NewEnquiry** and **SignModuleState** services. An operator can determine which mode the module is operating in using the KeySafe GUI or the command line utilities supplied with the module, or their own code - these operate outside the security boundary.

The modules must be accessed by a custom written application. Full documentation for the nCore API can be downloaded from the Thales web site.

nShield modules have on-board non-volatile memory. There are services that enable memory to be allocated as files. Files have Access Control Lists that determine what operations can be performed on their contents. nShield modules have on-board Real-time clock.

nShield modules include a technology called, the Secure Execution Environment (SEE). This enables operators to load a SEE machine. A SEE machine is operator written code that implements a specific Software Interrupt interface. This enables operators to implement non-cryptographic code in a protected memory space on the module that is outside the logical security boundary.

SEE code is executed in a protected environment. Whenever the SEE machine is running the nCore kernel is locked. Whenever the nCore kernel is active the SEE machine is locked. The SEE machine is excluded from the requirements of FIPS PUB 140-2.

The SEE machine has no direct access to objects stored on the module. In order to use cryptographic functions it must submit a job to the nCore kernel using the nCore API. The testing shows that the interface between the nCore kernel and the SEE machine is secure and that a malicious SEE machine cannot gain access to objects protected by the nCore kernel.

Before a operator can send commands to the SEE machine they must create an instance called a **SEE World**. A **SEE World** is treated as a separate operator by the module and must present the correct authentication before they can submit commands to the nCore kernel.

nShield modules are supplied with the SEE functions disabled. In order to use these functions the customer must purchase a feature-enable certificate enabling the functions for a specific module. The SEE feature is export controlled and therefore is not available in some territories.

All payShield modules are supplied with a SEE licence that enables them to run the Payshield secure payments processing library which supports a number of payments specific algorithms and functions which provide support for 3-D Secure, EMV (Europay, MasterCard, Visa) and PIN processing.

The module can be connected to a computer running one of the following operating systems:

- Windows
- Solaris
- HP-UX
- AIX
- Linux x86

Windows XP and Solaris were used to test the module for this validation.

## Chapter 2: Module Ports and Interfaces

The following table lists the logical interfaces to the module and how they map to physical interfaces.

| <b>Logical Interface</b> | <b>Physical Interface</b>  |
|--------------------------|--|
| Data In                  | PCI bus, Serial Interface, 16-way header   |
| Data Out                 | PCI bus, Serial Interface, 16-way header   |
| Control In               | PCI bus, Temperature Sensor, PSU Monitor, Reset Switch, Mode Switch, 16-way header |
| Status Out               | PCI bus, LED, Serial Interface, 16-way header                                      |
| Power                    | PCI bus  |

## Chapter 3: Excluded Components

The following components are excluded from FIPS 140-2 validation:

- Standard 64-bit PCI interface
- 9-way D-type Serial connector
- Mode switch
- Reset switch
- Status LED
- 16-way header
- DIP switches
- SEE machine
- Heat sink

## Chapter 4: Environmental Failure Protection

The nShield module offers protection from over and under voltage and over and under temperature.

The module is designed to operate in a PCI bus drawing power from the PCI 5V rail.

If the power on this rail fall below about 4.5V the PSU monitor shuts the module down, clearing all loaded keys. The PSU monitor will not allow the module to restart until sufficient voltage is applied, going through the standard power on procedure, including clearing all memory and performing all self tests.

If the voltage is increased to around 8V the power supply will continue to perform normally: drawing proportionally less current. Above 8.5V the power supply's over voltage protection device will trigger and all input power will be shorted to earth. This protect the module's cryptographic circuitry from damage. However, as the power supply is potted, it cannot be replaced and the module is therefore irreversibly destroyed.

The module has an on-board temperature sensor mounted close to the processors. If this sensor reaches seventy degrees centigrade or drops to zero degrees centigrade the module is put into its error state. The module turns off all communication on external buses and the Status LED flashes the Morse pattern SOS T (... --- ... -). The module can only be reset from an error state by turning the power supply off and back on - which for a PCI module means turning off power to the host computer. The module performs all normal power on procedures including clearing all memory and performing all self tests.

## Chapter 5: Roles

The module defines the following roles: Unauthenticated, User, nCipher Security Officer and Junior Security Officer. The nCipher Security Officer and Junior Security Officer roles are equivalent of FIPS 140-2 Crypto-Officer role.

### Unauthenticated

All connections are initially unauthenticated. If the module is initialized in level 3 mode, an unauthenticated operator is restricted to status commands, and commands required to complete authorization protocol.

### User

An operator enters the user role by providing the required authority to carry out a service. The exact accreditation required to perform each service is listed in the table of services.

In order to perform an operation on a stored key, the operator must first load the key blob. If the key blob is protected by a logical token, the operator must first load the logical token by loading shares from smart cards.

If the module is initialized in level 3 mode, the user role requires a certificate from the nCipher Security Officer to import or generate a new key. This certificate is linked to a token protected key.

Once an operator in the user role has loaded a key they can then use this key to perform cryptographic operations as defined by the Access Control List (ACL) stored with the key.

Each key blob contains an ACL that determines what services can be performed on that key. This ACL can require a certificate from a nCipher Security Officer authorizing the action. Some actions including writing tokens always require a certificate.

### nCipher Security Officer

The nCipher Security Officer (NSO) is responsible for overall security of the module.

The nCipher Security Officer is identified by a key pair, referred to as  $K_{NSO}$ . The hash of the public half of this key is stored when the unit is initialized. Any operation involving a module key or writing a token requires a certificate signed by  $K_{NSO}$ .

The nCipher Security Officer is responsible for creating the authentication tokens (smart cards) for each operator and ensuring that these tokens are physically handed to the correct person.

An operator assumes the role of NSO by loading the private half of  $K_{NSO}$  and presenting the **KeyID** for this key to authorize a command.

## Junior Security Officer

Where the nCipher Security Officer want to delegate responsibility for authorizing an action they can create a key pair and give this to their delegate who becomes a Junior Security Officer (JSO). An ACL can then refer to this key, and the JSO is then empowered to sign the certificate authorizing the action. The JSO's keys should be stored on a key blob protected by a token that is not used for any other purpose.

In order to assume the role of JSO, the operator loads the JSO key and presents the **KeyID** of this key, and if required the certificate signed by  $K_{NSO}$  that delegates authority to the key, to authorize a command.

A JSO can delegate portions of their authority to a new operator in the same way. The new operator will be a JSO if they have authority they can delegate, otherwise they will assume the user role.



## Chapter 6: Services available to each role

For more information on each of these services refer to the nShield Developer's Tutorial and nShield Developer's Reference.

The following services provide authentication or cryptographic functionality. The functions available depend on whether the operator is in the unauthenticated role, the user or junior security officer (JSO) roles, or the nCipher Security Officer (NSO) role. For each operation it lists the supported algorithms. Algorithms in square brackets are not under the operator's control. Algorithms used in optional portions of a service are listed in italics.

**Note** Algorithms marked with an asterisk are not approved by NIST. If the module is initialised in its level 3 mode, these algorithms are disabled. If module is initialized in level 2 mode, the algorithms are available. However, if you choose to use them, the module is not operating in FIPS approved mode.

| Key Access | Description  |
|------------|--|
| Create     | Creates a in-memory object, but does not reveal value.                                   |
| Erase      | Erases the object from memory, smart card or non-volatile memory without revealing value |
| Export     | Discloses a value, but does not allow value to be changed.                               |
| Report     | Returns status information   |
| Set        | Changes a CSP to a given value   |
| Use        | Performs an operation with an existing CSP - without revealing or changing the CSP       |

| Command / Service | Role   |               | Description   | Key/CSP access   | Key types  |   |
|-------------------|--------|---------------|---------------|--|--|---|
|                   | Unauth | JSO / User    |               |  |  | NSO   |
| Bignum Operation  | Yes    | Yes           | Yes           | Performs simple mathematical operations.   | No access to keys or CSPs  |   |
| Change Share PIN  | No     | pass phrase   | pass phrase   | Updates the pass phrase used to encrypt a token share. The pass phrase supplied by the operator is not used directly, it is first hashed and then combined with the module key. To achieve this the command decrypts the existing share using the old share key derived from old pass phrase, module key and smart card identity. It then derives a new share key based on new pass phrase, module key and smart card identity, erases old share from smart card and writes a new share encrypted under the new share key. | <i>Sets</i> the pass phrase for a share, <i>uses</i> module key, <i>uses</i> share key, <i>uses</i> module key, <i>creates</i> share key, <i>uses</i> new share key, <i>exports</i> encrypted share, <i>erases</i> old share | [SHA-1 and AES or Triple DES]                             |
| Channel Open      | No     | handle, ACL   | handle, ACL   | Opens a communication channel which can be used for bulk encryption or decryption. Channels using DES* or Triple DES in CBC mode use the Broadcom 5821 to perform the encryption.  | <i>Uses</i> a key object   | AES, DES*, Triple DES, Arc Four*, Aria*, Camellia*, SEED* |
| Channel Update    | No     | handle        | handle        | Performs encryption / decryption on a previously opened channel. The operation and key are specified in <b>ChannelOpen</b> .   | <i>Uses</i> a key object   | AES, DES*, Triple DES, Arc Four*, Aria*, Camellia*, SEED* |
| CheckUserACL      | No     | handle        | handle        | Determines whether the ACL associated with a key object allows a specific operator defined action.   | <i>Uses</i> a key object   |   |
| Clear Unit        | Yes    | Yes           | Yes           | Zeroizes all loaded keys, tokens and shares. Clear Unit does not erase long term keys, such as module keys.  | <i>Zeroizes</i> objects.   | All   |
| Create Buffer     | No     | cert [handle] | cert [handle] | Allocates an area of memory to load data. If the data is encrypted, this service specifies the encryption key and IV used. This service is feature enabled. The decrypt operation is performed by <b>LoadBuffer</b>  | <i>Uses</i> a key object   | AES, DES*, Triple DES, Arc Four*, Aria*, Camellia*, SEED* |

| Command / Service | Role   |                            | Description  | Key/CSP access  | Key types  |
|-------------------|--------|----------------------------|--|---|--|
|                   | Unauth | JSO / User<br>NSO          |  |   |  |
| Create SEE World  | No     | handle cert<br>handle cert | Creates a <b>SEE World</b> , passing in the initialization data stored in a buffer. This command checks the DSA signatures on the buffer using the public key provided. It also specifies whether debugging is allowed or not. Enabling debugging requires a certificate from the nCipher Security Officer.  | No access to keys or CSPs   |  |
| Decrypt           | No     | handle, ACL<br>handle, ACL | Decrypts a cipher text with a stored key returning the plain text.   | Uses a key object   | AES, DES <sup>*</sup> , Triple DES, Arc Four <sup>*</sup> , Aria <sup>*</sup> , Camellia <sup>*</sup> , SEED <sup>*</sup> , RSA <sup>*</sup> , ElGamal <sup>*</sup> , KCDSA <sup>*</sup>   |
| Derive Key        | No     | handle, ACL<br>handle, ACL | The <b>DeriveKey</b> service provides functions that the FIPS 140-2 standard describes as key wrapping and split knowledge - it does not provide key derivation in the sense understood by FIPS 140-2. Creates a new key object from a variable number of other keys already stored on the module and returns a handle for the new key. This service can be used to split, or combine, encryption keys. This service is used to wrap keys according to the KDP so that a key server can distribute the wrapped key to micro-HSM devices. | <i>Uses</i> a key object, create a new key object.                          | AES, AES key wrap, RSA, EC-DH, EC_MQV, Triple DES, PKCS #8 <sup>*</sup> , TLS key derivation, XOR, DLIES (D/H plus Triple DES or D/H plus AES), Aria <sup>*</sup> , Arc Four <sup>*</sup> , Camellia <sup>*</sup> , DES <sup>*</sup> , SEED <sup>*</sup> |
| Destroy           | No     | handle<br>handle           | Removes an object, if an object has multiple handles as a result of <b>RedeemTicket</b> service, this removes the current handle.  | <i>Erases</i> a lmpath, <b>SEEWORLD</b> , logical token, or any key object. | All  |
| Duplicate         | No     | handle, ACL<br>handle, ACL | Creates a second instance of a key object with the same ACL and returns a handle to the new instance.  | <i>Creates</i> a new key object.  | All  |

| Command / Service              | Role         |             | Description | Key/CSP access   | Key types   |  |
|--------------------------------|--------------|-------------|-------------|--|---|--|
|                                | Unauth       | JSO / User  |             |  |   | NSO  |
| Encrypt                        | No           | handle, ACL | handle, ACL | Encrypts a plain text with a stored key returning the cipher text.   | Uses a key object                                     | AES, DES <sup>*</sup> , Triple DES, RSA <sup>*</sup> , ElGamal <sup>*</sup> , Arc Four <sup>*</sup> , Aria <sup>*</sup> , Camellia <sup>*</sup> , SEED <sup>*</sup> , KCDSA <sup>*</sup> |
| Erase File                     | level 2 only | cert        | yes         | Removes a file, but not a logical token, from a smart card or software token.  | No access to keys or CSPs                             |  |
| Erase Share                    | level 2 only | cert        | yes         | Removes a share from a smart card or software token.   | Erases a share  |  |
| Existing Client                | yes          | yes         | yes         | Starts a new connection as an existing client.   | No access to keys or CSPs                             |  |
| Export                         | No           | handle, ACL | handle, ACL | If the unit is operating in FIPS level 2 mode this operation is only available for public keys - see Operating a level 2 module in FIPS mode on page 41. If the unit has been initialized to comply with FIPS 140-2 level 3 roles and services and key management, this service is only available for public keys. | Exports a [public] key object.                        | Any key type   |
| Feature Enable                 | No           | cert        | cert        | Enables a service. This requires a certificate signed by the Master Feature Enable key.  | Uses the public half of the Master Feature Enable Key | [DSA]  |
| Firmware Authenticate          | yes          | yes         | yes         | Reports firmware version. Performs a zero knowledge challenge response protocol based on HMAC that enables an operator to ensure that the firmware in the module matches the firmware supplied by Thales. The protocol generates a random value to use as the HMAC key.  | No access to keys or CSPs                             | HMAC   |
| Foreign Token Command (Bypass) | No           | handle      | handle      | Sends an ISO-7816 command to a smart card over the channel opened by <b>ForeignTokenOpen</b> .   | Uses a bypass channel.                                |  |

| Command / Service           | Role         |            | Description | Key/CSP access   | Key types   |  |
|-----------------------------|--------------|------------|-------------|--|---|--|
|                             | Unauth       | NSO / User |             |  |   |  |
| Foreign Token Open (Bypass) | No           | FE, cert   | FE          | Opens a channel to foreign smart card that accepts ISO-7816 commands. This service cannot be used if the smart card has been formatted using <b>FormatToken</b> . The channel is closed when the card is removed from the reader, or if the handle is destroyed.<br>This service is feature enabled. | <i>Creates</i> a bypass channel.  |  |
| FormatToken                 | level 2 only | cert       | yes         | Formats a smart card or software token ready for use.  | May <i>use</i> a module key to create challenge response value  | [AES, Triple DES]  |
| Generate Key                | level 2 only | cert       | yes         | Generates a symmetric key of a given type with a specified ACL and returns a handle. Optionally returns a certificate containing the ACL.  | <i>Creates</i> a new symmetric key object. <i>Sets</i> the ACL and Application data for that object. Optionally <i>uses</i> module signing key and <i>exports</i> the key generation certificate. | AES, Triple DES, Arc Four*, Aria*, Camellia*, DES*, SEED*.                     |
| Generate Key Pair           | level 2 only | cert       | yes         | Generates a key pair of a given type with specified ACLs for each half or the pair. Performs a pair wise consistency check on the key pair. Returns two key handles. Optionally returns certificates containing the ACL.   | <i>Creates</i> two new key objects. <i>Sets</i> the ACL and Application data for those objects. Optionally <i>uses</i> module signing key and <i>exports</i> two key generation certificates.     | Diffie-Hellman, DSA, DSA2, ECDSA, ECDSA2, EC-DH, EC-MQV, RSA, ElGamal*, KCDSA* |
| Generate KLF                | No           | FE         | FE          | Generates a new long term key.   | <i>Erases</i> the module long term signing key, <i>creates</i> new module long term signing key.  | [DSA and ECDSA]  |
| Generate Logical Token      | level 2 only | cert       | yes         | Creates a new logical token, which can then be written as shares to smart cards or software tokens   | <i>Uses</i> module key. <i>Creates</i> a logical token.   | [AES or Triple DES]  |

| Command / Service               | Role   |                            | Description  | Key/CSP access  | Key types   |              |
|---------------------------------|--------|----------------------------|--|---|---|--------------|
|                                 | Unauth | JSO / User<br>NSO          |  |   |   |              |
| Get ACL                         | No     | handle, ACL<br>handle, ACL | Returns the ACL for a given handle.                    | <i>Exports</i> the ACL for a key object.  |   |              |
| Get Application Data            | No     | handle, ACL<br>handle, ACL | Returns the application information stored with a key. | <i>Exports</i> the application data of a key object.  |   |              |
| Get Challenge                   | yes    | yes                        | yes  | Returns a random nonce that can be used in certificates   | No access to keys or CSPs   |              |
| Get Key Info                    | No     | handle                     | handle   | Superseded by <b>GetKeyInfoExtended</b> retained for compatibility.   | <i>Exports</i> the SHA-1 hash of a key object                         |              |
| Get Key Info Extended           | No     | handle                     | handle   | Returns the hash of a key for use in ACLs   | <i>Exports</i> the SHA-1 hash of a key object                         |              |
| Get Logical Token Info          | No     | handle                     | handle   | Superseded by <b>GetLogicalTokenInfoExtended</b> retained for compatibility.  | <i>Exports</i> the SHA-1 hash of a logical token.                     | [SHA-1]      |
| Get Logical Token Info Extended | No     | handle                     | handle   | Returns the token hash and number of shares for a logical token   | <i>Exports</i> the SHA-1 hash of a logical token.                     | [SHA-1]      |
| Get Module Keys                 | yes    | yes                        | yes  | Returns a hashes of the nCipher Security Officer's key and all loaded module keys.  | <i>Exports</i> the SHA-1 hash of KNSO and module keys.                | [SHA-1]      |
| Get Module Long Term Key        | yes    | yes                        | yes  | Returns a handle to the public half of the module's signing key. this can be used to verify key generation certificates and to authenticate inter module paths. | <i>Exports</i> the public half of the module's long term signing key. | [DSA, ECDSA] |
| Get Module Signing Key          | yes    | yes                        | yes  | Returns the public half of the module's signing key. This can be used to verify certificates signed with this key.  | <i>Exports</i> the public half of the module's signing key.           | [DSA2]       |
| Get RTC                         | yes    | yes                        | yes  | Reports the time according to the on-board real-time clock  | No access to keys or CSPs   |              |
| Get Share ACL                   | yes    | yes                        | yes  | Returns the access control list for a share   | <i>Exports</i> the ACL for a token share on a smart card.             |              |

| Command / Service          | Role   |            | Description | Key/CSP access   | Key types   |
|----------------------------|--------|------------|-------------|--|---|
|                            | Unauth | JSO / User |             |  |   |
| GetSlot Info               | yes    | yes        | yes         | Uses a module key if token is formatted with a challenge response value. | [AES, Triple DES]   |
| Get Slot List              | yes    | yes        | yes         | No access to keys or CSPs  |   |
| GetTicket                  | No     | handle     | handle      | Uses a key object, logical token, Impath, SEEWORLD.                      |   |
| Get World Signers          | No     | handle     | handle      | Uses a SEEWORLD object.  |   |
| Hash                       | yes    | yes        | yes         | No access to keys or CSPs  | HSA-160*, MD5*, RIPEMD 160*, SHA-1, SHA-256, SHA-384, SHA-512 |
| Impath Get Info            | No     | handle     | handle      | Uses an Impath, exports status information.                              |   |
| Impath Key Exchange Begin  | FE     | FE         | FE          | Creates a set of Impath keys   | [DSA2 or DSA and Diffie Hellman] AES, Triple-DES              |
| Impath Key Exchange Finish | No     | handle     | handle      | Creates a set of Impath keys.  | [DSA2 or DSA and Diffie Hellman, AES, Triple-DES]             |
| Impath Receive             | No     | handle     | handle      | Uses an Impath key.  | [AES or Triple DES]   |
| Impath Send                | No     | handle     | handle      | Uses an Impath key.  | [AES or Triple DES]   |

| Command / Service  | Role         |                   | Description   | Key/CSP access  | Key types   |
|--------------------|--------------|-------------------|---|---|---|
|                    | Unauth       | JSO / User<br>NSO |   |   |   |
| Import             | level 2 only | cert<br>yes       | <p>Loads a key and ACL from the host and returns a handle.</p> <p>If the unit is operating in FIPS mode at level 2, this operation must only be used for public keys - see Operating a level 2 module in FIPS mode on page 41</p> <p>If the unit has been initialized to comply with FIPS 140-2 level 3 roles and services and key management, this service is only available for public keys.</p>  | Creates a new key object to store imported key, sets the key value, ACL and App data. | Any key type  |
| Initialise         | init         | init<br>init      | <p>Initializes the module, returning it to the factory state. This clears all NVRAM files, all loaded keys and all module keys and the module signing key.</p> <p>It also generates a new KMO and module signing key.</p> <p>The only key that is not zeroized is the long term signing key. This key only serves to provide a cryptographic identity for a module that can be included in a PKI certificate chain. Thales may issue such certificates to indicate that a module is a genuine nShield module. This key is not used to encrypt any other data.</p> | Erases keys, Creates KMO and KML  | [DSA2]  |
| Load Blob          | No           | handle<br>handle  | Loads a key that has been stored in a key blob. The operator must first have loaded the token or key used to encrypt the blob.  | Uses module key, logical token, or archiving key, creates a new key object.           | Triple DES and SHA-1 or AES, DH, or RSA plus AES, SHA-1, and HMAC SHA-1 |
| Load Buffer        | No           | handle<br>handle  | <p>Loads signed data into a buffer. Several load buffer commands may be required to load all the data, in which case it is the responsibility of the client program to ensure they are supplied in the correct order.</p> <p>Requires the handle of a buffer created by <b>CreateBuffer</b>.</p>  | No access to keys or CSPs   |   |
| Load Logical Token | yes          | yes<br>yes        | <p>Allocates space for a new logical token - the individual shares can then be assembled using <b>ReadShare</b> or <b>ReceiveShare</b>. Once assembled the token can be used in <b>LoadBlob</b> or <b>MakeBlob</b> commands.</p>  | Uses module key   | [AES or Triple DES]   |



| Command / Service | Role   |                   | Description  | Key/CSP access   | Key types  |
|-------------------|--------|-------------------|--|--|--|
|                   | Unauth | NSO<br>JSO / User |  |  |  |
| Make Blob         | No     | handle, ACL       | Creates a key blob containing the key and returns it. The key object to be exported may be any algorithm.  | <i>Uses</i> module key, logical token or archiving key, <i>exports</i> encrypted key object. | Triple DES and SHA-1 or AES, DH, or RSA plus AES, SHA-1, and HMAC SHA-256 or SHA-1 |
| Mod Exp           | yes    | yes               | Performs a modular exponentiation on values supplied with the command.   | No access to keys or CSPs  |  |
| Mod Exp CRT       | yes    | yes               | Performs a modular exponentiation on values, supplied with the command using Chinese Remainder Theorem.  | No access to keys or CSPs  |  |
| Module Info       | yes    | yes               | Reports low level status information about the module. This service is designed for use in Thales's test routines.   | No access to keys or CSPs  |  |
| NewClient         | yes    | yes               | Returns a client id.   | No access to keys or CSPs  |  |
| New Enquiry       | yes    | yes               | Reports status information.  | No access to keys or CSPs  |  |
| No Operation      | yes    | yes               | Does nothing, can be used to determine that the module is responding to commands.  | No access to keys or CSPs  |  |
| NVMem Allocate    | No     | cert              | Allocates an area of non-volatile memory as a file and sets the ACLs for this file. This command can now be used to write files protected by an ACL to a smart card  | No access to keys or CSPs  |  |
| NVMem Free        | No     | cert              | Frees a file stored in non-volatile memory. This command can now be used to write files protected by an ACL to a smart card  | No access to keys or CSPs  |  |
| NVMem List        | yes    | yes               | Reports a list of files stored in the non-volatile memory. This command can now be used to list files protected by an ACL on a smart card  | No access to keys or CSPs  |  |
| NVMem Operation   | No     | cert, ACL         | Performs an operation on a file stored in non-volatile memory. Operations include: read, write, increment, decrement, etc. This command can now be used to write files protected by an ACL to a smart card | No access to keys or CSPs  |  |

| Command / Service | Role    |                         | Description             | Key/CSP access  | Key types  |
|-------------------|---------|-------------------------|-------------------------|---|--|
|                   | Unauth  | JSO / User              |                         |   |  |
| Random Number     | yes     | yes                     | yes                     | Uses DRBG key.  | [AES]  |
| Random Prime      | yes     | yes                     | yes                     | Uses DRBG key.  | [AES]  |
| Read File         | level 2 | cert                    | yes                     | Reads a file, but not a logical token, from a smart card or software token. This command can only read files without ACLs.  | No access to keys or CSPs  |
| Read Share        | yes     | yes                     | yes                     | Reads a share from a physical token. Once sufficient shares have been loaded recreates token- may require several <b>ReadShare</b> OR <b>ReceiveShare</b> commands.                 | Uses pass phrase, module key, creates share key, uses share key, creates a logical token.                    |
| Receive Share     | No      | handle, encrypted share | handle, encrypted share | Takes a share encrypted with <b>SendShare</b> and a pass phrase and uses them to recreate the logical token. - may require several <b>ReadShare</b> OR <b>ReceiveShare</b> commands | Uses an Impath key, uses pass phrase, module key, creates share key, uses share key, creates a logical token |
| Redeem Ticket     | No      | ticket                  | ticket                  | Gets a handle in the current name space for the object referred to by a ticket created by <b>GetTicket</b> .  | Uses a key object, logical token, Impath, or <b>SEEWORLD</b> .   |
| Remove KM         | No      | cert                    | yes                     | Removes a loaded module key.  | Erases a module key  |

| Command / Service         | Role   |             | Description | Key/CSP access   | Key types  |   |
|---------------------------|--------|-------------|-------------|--|--|---|
|                           | Unauth | JSO / User  |             |  |  | NSO   |
| SEE Job                   | No     | cert        | yes         | Sends a command to a <b>SEE World</b> .  | No access to keys or CSPs                          |   |
| Set ACL                   | No     | handle, ACL | handle, ACL | Sets the ACL for an existing key. The existing ACL for the key must allow the operation.   | Sets the Access Control List for a key object      |   |
| Set Application Data      | No     | handle, ACL | handle, ACL | Stores information with a key.   | Sets the application data stored with a key object |   |
| Set KM                    | No     | cert        | yes         | Loads a key object as a module key.  | Uses a key object, sets a module key               | AES, Triple DES   |
| Set NSO Perm              | init   | init        | No          | Loads a key hash as the nCipher Security Officer's Key and sets the security policy to be followed by the module. This can only be performed while the unit is in the initialisation state.  | Sets the nCipher Security officer's key hash.      | [SHA-1 hash of DSA key]                                     |
| Set RTC                   | No     | cert        | yes         | Sets the real-time clock.  | No access to keys or CSPs                          |   |
| Set SEE Machine           | No     | cert handle | handle      | Loads the contents of a buffer (created by <b>CreateBuffer</b> / <b>LoadBuffer</b> ) as the SEE machine for this module. This command checks the signatures on the buffer. The SEE machine is excluded from the cryptographic boundary, when the module is running in FIPS mode. | Uses the key provided in buffer                    | DSA, DSA2, Triple DES MAC, HMAC                             |
| Sign                      | No     | handle, ACL | handle, ACL | Returns the digital signature or MAC of plain text using a stored key.   | Uses a key object                                  | RSA, DSA, DSA2, ECDSA, ECDSA2, Triple DES MAC, HMAC, KCDSA* |
| Sign Module State         | No     | handle, ACL | handle, ACL | Signs a certificate describing the modules security policy, as set by SetNSOPerm   | Uses the module signing key                        | [DSA]   |
| Send Share                | No     | handle, ACL | handle, ACL | Reads a logical token share and encrypts it under an impath key for transfer to another module where it can be loaded using <b>ReceiveShare</b>  | Uses an Impath key, exports encrypted share.       | [AES, Triple DES]   |
| Statistics Enumerate Tree | yes    | yes         | yes         | Reports the statistics available.  | No access to keys or CSPs                          |   |

| Command / Service  | Role    |             | Description | Key/CSP access   | Key types   |   |
|--|---------|-------------|-------------|--|---|---|
|  | Unauth  | JSO / User  |             |  |   | NSO   |
| Statistic Get Value  | yes     | yes         | yes         | Reports a particular statistic.  | No access to keys or CSPs   |   |
| Trace SEE World  | No      | cert        | yes         | Reports debugging output from a <b>SEE World</b> .   | No access to keys or CSPs   |   |
| Update Firmware Service<br>(Calls<br>Programming Begin<br>Programming Begin Chunk<br>Programming Load Block<br>Programming End Chunk<br>Programming End) | monitor | monitor     | monitor     | <p>These commands are used in the update firmware service.</p> <p>The individual commands are required to load the candidate firmware image in sections small enough to be transported by the interface.</p> <p>Thales supply the <b>LoadROM</b> utility for the administrator to use for this service. This utility issues the correct command sequence to load the new firmware.</p> <p>The module will only be operating in a FIPS approved mode if you install firmware that has been validated by NIST / CSEC.</p> <p>Administrators who require FIPS validation should only upgrade firmware after NIST / CSEC issue a new certificate.</p> <p>The monitor also checks that the Version Sequence Number (VSN) of the firmware is as high or higher than the VSN of the firmware currently installed.</p> | <p><i>Uses</i> Firmware Integrity Key and Firmware Confidentiality Keys.</p> <p><i>Sets</i> Firmware Integrity Key and Firmware Confidentiality Keys.</p>   | [DSA2, AES]   |
| Verify   | No      | handle, ACL | handle, ACL | Verifies a digital signature using a stored key.   | <i>Uses</i> a key object.   | RSA, DSA, DSA2, ECDSA, ECDSA2, Triple DES MAC, HMAC, KCDSA* |
| Write File   | level 2 | cert        | yes         | Writes a file, but not a logical token, to a smart card or software token.<br>Note these files do not have an ACL, use the NVMEM commands to create files with an ACL.   | No access to keys or CSPs   |   |
| Write Share  | No      | cert handle | handle      | Writes a new share to a smart card or software token. The number of shares that can be created is specified when the token is created. All shares must be written before the token is destroyed.   | <i>Sets</i> pass phrase, <i>uses</i> module key, <i>creates</i> share, <i>uses</i> pass phrase and module key, <i>creates</i> share key, <i>uses</i> module key, <i>uses</i> share key, <i>exports</i> encrypted share. | [AES, Triple DES, SHA-1]                                    |

## Terminology

| Code            | Description  |
|-----------------|--|
| No              | The operator can not perform this service in this role.  |
| yes             | The operator can perform this service in this role without further authorization.  |
| handle          | <p>The operator can perform this service if they possess a valid handle for the resource: key, channel, impath, token, buffers, <b>SEWorld</b>.</p> <p>The handle is an arbitrary number generated when the object is created.</p> <p>The handle for an object is specific to the operator that created the object.</p> <p>The ticket services enable an operator to pass an ID for an object they have created to another operator or <b>SEWorld</b>.</p>   |
| ACL             | <p>The operator can only perform this service with a key if the ACL for the key permits this service. The ACL may require that the operator present a certificate signed by a Security Officer or another key.</p> <p>The ACL may specify that a certificate is required, in which case the module verifies the signature on the certificate before permitting the operation.</p>  |
| pass phrase     | An operator can only load a share, or change the share PIN, if they possess the pass phrase used to derive the share. The module key with which the pass phrase was combined must also be present.   |
| cert            | An operator can only perform this service if they are in possession of a certificate from the nCipher Security Officer. This certificate will reference a key. The module verifies the signature on the certificate before permitting the operation.   |
| FE              | This service is not available on all modules. It must be enabled using the <b>FeatureEnable</b> service before it can be used.   |
| level 2 only    | <p>These services are available to the unauthenticated operator only when the module is initialized in it FIPS 140-2 level 2 mode. The module can be initialized to comply with FIPS 140-2 level 3 roles and services and key management by setting the <b>FIPS_level3_compliance</b> flag. If this flag is set: the <b>Generate Key</b>, <b>Generate Key Pair</b> and <b>Import</b> commands require authorization with a certificate signed by the nCipher Security Officer.</p> <p>the <b>Import</b> command fails if you attempt to import a key of a type that can be used to <b>Sign</b> or <b>Decrypt</b> messages.</p> <p>the <b>GenerateKey</b>, <b>GenerateKeyPair</b>, <b>Import</b> and <b>DeriveKey</b> operations will not allow you to create an ACL for a secret key that allows the key to be exported in plain text.</p> |
| encrypted share | The <b>ReceiveShare</b> command requires a logical token share encrypted using an Impath key created by the <b>SendShare</b> command.  |
| ticket          | The <b>RedeemTicket</b> command requires the ticket generated by <b>GetTicket</b> .  |
| init            | These services are used to initialise the module. They are only available when the module is in the initialisation mode. To put the module into initialisation mode you must have physical access to the module and put the mode switch into the initialisation setting. In order to restore the module to operational mode you must put the mode switch back to the Operational setting.  |
| monitor         | These services are used to reprogram the module. They are only available when the module is in the monitor mode. To put the module into monitor mode you must have physical access to the module and put the mode switch into the monitor setting. In order to restore the module to operational mode you reinitialize the module and then return it to operational state.   |

## Chapter 7: Keys

For each type of key used by the nShield modules, the following section describes the access that a operator has to the keys.

nShield modules refer to keys by their handle, an arbitrary number, or by its SHA-1 hash.

### nCipher Security Officer's key

The nCipher Security officer's key must be set as part of the initialisation process. This is a public / private key pair that the nCipher Security Officer uses to sign certificates to authorize key management and other secure operations.

The SHA-1 hash of the public half of this key pair is stored in the module EEPROM.

The public half of this key is included as plain text in certificates.

The module treats anyone in possession of the private half of this key as the nCipher Security Officer.

If you use the standard tools supplied by Thales to initialise the module, then this key is a DSA key stored as a key blob protected by a logical token on the Administrator Card Set.

### Junior Security Officer's key

Because the nCipher Security Officer's key has several properties, it is good practice to delegate authority to one or more Junior Security Officers, each with authority for defined operations.

To create a Junior Security Officer (JSO) the NSO creates a certificate signing key for use as their JSO key. This key must be protected by a logical token in the same manner as any other application key.

Then to delegate authority to the JSO, the nCipher Security Officer creates a certificate containing an Access Control List specifying the authority to be delegated and the hash of the JSO key to which the powers are to be delegated.

The JSO can then authorize the actions listed in the ACL - as if they were the NSO - by presenting the JSO key and the certificate. If the JSO key is created with the Sign permission in its ACL, the JSO may delegate parts of their authority to another key. The holder of the delegate key will need to present the certificate signed by the NSO and the certificate signed by the JSO. If the JSO key only has **UseAsCertificate** permissions, then they cannot delegate authority.

If you use the standard tools supplied by Thales to initialise the module, then this key is a DSA key stored as a key blob protected by a logical token on the Administrator Card Set.

## Long term signing key

The nShield modules store one 160-bit and one 256-bit random number in the EEPROM.

The 160-bit number is combined with a discrete log group stored in the module firmware to produce a DSA key. The 256-bit number is used as the private exponent of a ECDSA key using the NIST P521 curve.

This key can be reset to a new random value by the **GenerateKLF** service. It can be used to sign a module state certificate using the **SignModuleState** service and the public value retrieved by the non-cryptographic service **GetLongTermKey**.

This is the only key that is not zeroized when the module is initialized.

This key is not used to encrypt any other data. It only serves to provide a cryptographic identity for a module that can be included in a PKI certificate chain. Thales may issue such certificates to indicate that a module is a genuine Thales module.

## Module signing key

When the nShield module is initialized it automatically generates a 3072-bit DSA2 key pair that it uses to sign certificates. Signatures with this key use SHA-256. The private half of this pair is stored internally in EEPROM and never released. The public half is revealed in plaintext, or encrypted as a key blob. This key is only ever used to verify that a certificate was generated by a specified module.

## Module keys

Module keys are AES or Triple DES used to protect tokens. The nShield modules generates the first module key  $K_{M0}$  when it is initialized. This module key is guaranteed never to have been known outside this module.  $K_{M0}$  is an AES key. The nCipher Security Officer can load further module keys. These can be generated by the module or may be loaded from an external source. Setting a key as a module key stores the key in EEPROM.

Module keys can not be exported once they have been assigned as module keys. They may only be exported on a key blob when they are initially generated.

## Logical tokens

A logical token is an AES or Triple DES key used to protect key blobs. Logical tokens are associated with module keys. The key type depends on the key type of the module key.

When you create a logical token, you must specify parameters, including the total number of shares, and the number of shares required to recreate the token, the quorum. The total number can be any integer between 1 and 64 inclusive. The quorum can be any integer from 1 to the total number.

A logical token is always generated randomly, using the on-board random number generator.

While loaded in the module logical tokens are stored in the object store.

Token keys are never exported from the module, except on physical tokens or software tokens. When a module key is exported the logical token - the Triple DES key plus the token parameters - is first encrypted with a module key. Then the encrypted token is split into shares using the Shamir Threshold Sharing algorithm, even if the total number of shares is one. Each share is then encrypted using a share key and written to a physical token - a smart card - or a software token. Logical tokens can be shared between one or more physical token. The properties for a token define how many shares are required to recreate the logical token. Shares can only be generated when a token is created. The firmware prevents a specific share from being written more than once.

Logical tokens are not used for key establishment.

## Share Key

A share key is used to protect a logical token share when they are written to a smart card or software token that is used for authentication. The share key is created by creating a message comprised of a secret prefix, Module key, Share number, smart card unique id and an optional 20 bytes supplied by the operator (expected to be the SHA-1 hash of a pass phrase entered into the application), and using this as the input to a PRNG function to form a unique key used to encrypt the share - this is either an AES or Triple DES key depending on the key type of the logical token which is itself determined by the key type of the module key. This key is not stored on the module. It is recalculated every time share is loaded. The share data includes a MAC, if the MAC does not verify correctly the share is rejected.

The share key is not used directly to protect CSPs nor is the Share Key itself considered a CSP. It is used for authentication only. The logical token needs to be reassembled from the shares using Shamir Threshold Sharing Scheme and then be decrypted using the module key. Only then can the logical token be used to decrypt application keys.



## Impath keys

An impath is a secure channel between two modules.

To set up an impath two modules perform a key-exchange, using Diffie-Hellman.

The Diffie Hellman operations has been validated in CVL Cert. #1. The CVL Cert. #1 is not fully compliant to SP 800-56A as the key derivation function has not been tested.

The key exchange parameters for each module are signed by that module's signing key. Once the modules have validated the signatures the module derives four symmetric keys for cryptographic operations.

Currently symmetric keys are AES or Triple DES. AES is used if both modules use 2.50.16 or later firmware, Triple DES is used where the other module is running older firmware. The four keys are used for encryption, decryption, MAC creation, MAC validation. The protocol ensures that the key Module 1 uses for encryption is used for decryption by module 2.

## Key objects

Keys used for encryption, decryption, signature verification and digital signatures are stored in the module as objects in the object store in RAM. All key objects are identified by a random identifier that is specific to the operator and session.

All key objects are stored with an Access control List or ACL. The ACL specifies what operations can be performed with this key. Whenever an operator generates a key or imports a key in plain text they must specify a valid ACL for that key type. The ACL can be changed using the **SetACL** service. The ACL can only be made more permissive if the original ACL includes the **ExpandACL** permission.

Key objects may be exported as key blobs if their ACL permits this service. Each blob stores a single key and an ACL. The ACL specifies what operations can be performed with this copy of the key. The ACL stored with the blob must be at least as restrictive as the ACL associated with the key object from which the blob was created. When you load a key blob, the new key object takes its ACL from the key blob. Working key blobs are encrypted under a logical token. Key objects may also be exported as key blobs under an archiving key. The key blob can be stored on the host disk or in the module NVRAM.

Key objects can only be exported in plain text if their ACL permits this operation. If the module has been initialized to comply with FIPS 140-2 level 3 roles and services and key management the ACL for a private or secret key cannot include the export as plain service. An operator may pass a key to another operator - or to a SEE World - using the ticketing mechanism. The **GetTicket** mechanism takes a key identifier and returns a ticket. This ticket refers to the key identifier - it does not include any key data. A ticket can be passed as a byte block to the other

operator who can then use the **RedeemTicket** service to obtain a key identifier for the same object that is valid for their session. As the new identifier refers to the same object the second operator is still bound by the original ACL.

## Session keys

Keys used for a single session are generated as required by the module. They are stored along with their ACL as objects in the object store. These may be of any supported algorithm.

## Archiving keys

It is sometimes necessary to create an archive copy of a key, protected by another key. Keys may be archived using:

- Three-key Triple DES keys (used for unwrapping legacy keys and wrapping public keys only).
- A combination of three-key Triple DES and RSA keys (unwrapping legacy keys only).  
In this case a random 168-bit Triple DES key is created which is used to encrypt working key and then this key is wrapped by the RSA key.
- A scheme using RSA.  
3072-bit RSA is used to establish a secret from which encryption keys are generated. The holders of the public and private halves of the RSA key must already exist in the module as operators.  
The keys generated are either AES or Triple-DES keys, for the purpose of protecting other keys. AES is used by default as of firmware version 2.50.16. (with Triple-DES available for legacy purposes).  
Once the key agreement process is complete, the module uses an additional keyed hashing process to protect the integrity of the nCore Key object to be archived, which is comprised of the key type, key value and Access Control List. This process uses HMAC SHA-256 by default. (with HMAC SHA-1 available for legacy purposes).
- A scheme using Diffie Hellman:  
3072-bit Diffie-Hellman, which is allowed for use in the Approved mode, is used to establish a secret from which encryption keys are generated. Both parties in the Diffie-Hellman key agreement process exist in the module as operators. The keys generated are either AES or Triple-DES keys, for the purpose of protecting other keys. AES is used by

default as of firmware version 2.50.16. (with Triple-DES available for legacy purposes). Please note that the Diffie-Hellman private key must be stored externally on the smartcard, if the archived keys are to be retrieved at a later time.

Once the key agreement process is complete, the module uses an additional keyed hashing process to protect the integrity of the nCore Key object to be archived, which is comprised of the key type, key value and Access Control List. This process uses HMAC SHA-256 by default. (with HMAC SHA-1 available for legacy purposes).

Although provided by the firmware, this option is currently not used by any Thales tools. Other third party applications external to the module, may take advantage of this option, at the discretion of the developer.

When a key is archived in this way it is stored with its ACL

When you generate or import the archiving key, you must specify the **UseAsBlobKey** option in the ACL. The archiving key is treated as any other key object.

When you generate or import the key that you want to archive you must specify the Archival options in the ACL. This options can specify the hash(es) of the allowed archiving key(s). If you specify a list of hashes, no other key may be used.

## Certificate signing keys

The ACL associated with a key object can call for a certificate to be presented to authorize the action. The required key can either be the nCipher Security Officer's key or any other key. Keys are specified in the ACL by an identifying key SHA-1 hash. The key type is also specified in the ACL although DSA is standard, any signing algorithm may be used, all Thales tools use DSA.

Certain services can require certificates signed by the nCipher Security Officer.

## Firmware Integrity Key

All firmware is signed using a 3072-bit DSA2 key pair. Signatures with this key use SHA-256.

The module checks the signature before new firmware is written to flash. A module only installs new firmware if the signature decrypts and verifies correctly.

The private half of this key is stored at Thales.

The public half is included in all firmware. The firmware is stored in flash memory when the module is switched off, this is copied to RAM as part of the start up procedure.

## **Firmware Confidentiality Key**

All firmware is encrypted using AES to prevent casual decompilation.

The encryption key is stored at Thales's offices and is in the firmware.

The firmware is stored in flash memory when the module is switched off, this is copied to RAM as part of the start up procedure.

## **Master Feature Enable Key**

For commercial reasons not all nShield modules offer all services. Certain services must be enabled separately. In order to enable a service the operator presents a certificate signed by the Master Feature Enable Key. This causes the module to set the appropriate bit in the EEPROM.

The Master Feature Enable Key is a DSA key pair. The private half of this key pair is stored at Thales's offices. The public half of the key pair is included in the firmware. The firmware is stored in flash memory when the module is switched off, this is copied to RAM as part of the start up procedure.

## **DRBG Key**

The module uses the CTR\_DRBG from SP800-90 with a 256-bit AES key. This key is seeded from the on board entropy source whenever the module is initialised and is reseeded according to SP800-90 with a further 512-bits of entropy after every 2048-bytes of output. This key is only ever used by the DRBG. It is never exposed outside the module.

## Chapter 8: Rules

### Identification and authentication

Communication with the nShield modules is performed via a server program running on the host machine, using standard inter process communication, using sockets in UNIX operating systems, named pipes under Windows.

In order to use the module the operator must first log on to the host computer and start an nShield enabled application. The application connects to the hardware, this connection is given a client ID, a 32-bit arbitrary number.

Before performing any service the operator must present the correct authorization. Where several stages are required to assemble the authorization, all the steps must be performed on the same connection. The authorization required for each service is listed in the section Services available to each role on page 17. An operator cannot access any service that accesses CSPs without first presenting a smart card, or software token.

The nShield modules performs identity based authentication. Each individual operator is given a smart card that holds their authentication data - the logical token share - in an encrypted form. All operations require the operator to first load the logical token from their smart card.

### Access Control

Keys are stored on the host computer's hard disk in an encrypted format, known as a key blob. In order to load a key the operator must first load the token used to encrypt this blob.

Tokens can be divided into shares. Each share can be stored on a smart card or software token on the computer's hard disk. These shares are further protected by encryption with a pass phrase and a module key. Therefore an operator can only load a key if they possess the physical smart cards containing sufficient shares in the token, the required pass phrases and the module key are loaded in the module.

Module keys are stored in EEPROM in the module. They can only be loaded or removed by the nCipher Security Officer, who is identified by a public key pair created when the module is initialized. It is not possible to change the nCipher Security Officer's key without re initializing the module, which clears all the module keys, thus preventing access to all other keys.

The key blob also contains an Access Control List that specifies which services can be performed with this key, and the number of times these services can be performed. These can be hard limits or per authorization limits. If a hard limit is reached that service can no longer be performed on that key. If a per-authorization limit is reached the operator must reauthorize the key by reloading the token.

All objects are referred to by handle. Handles are cross-referenced to **ClientIDs**. If a command refers to a handle that was issued to a different client, the command is refused. Services exist to pass a handle between **ClientIDs**.

## Access Control List

All key objects have an Access Control List (ACL). The operator must specify the ACL when they generate or import the key. The ACL lists every operation that can be performed with the key - if the operation is not in the ACL the module will not permit that operation. In particular the ACL can only be altered if the ACL includes the **SetACL** service. The ACL is stored with the key when it is stored as a blob and applies to the new key object created when you reload the blob.

The ACL can specify limits on operations - or groups of operations - these may be global limits or per authorization limits. If a global limit is exceeded then the key cannot be used for that operation again. If a per authorization limit is exceeded then the logical token protecting the key must be reloaded before the key can be reused.

An ACL can also specify a certifier for an operation. In this case the operator must present a certificate signed by the key whose hash is in the ACL with the command in order to use the service.

An ACL can also list Operator Defined actions. These actions do not permit any operations within the module, but can be tested with the **CheckUserAction** service. This enables SEE programs to make use of the ACL system for their own purposes. For example payShield uses this feature to determine the role of a Triple-DES key within EMV.

An ACL can also specify a host service identifier. In which case the ACL is only met if the hardserver appends the matching Service name. This feature is designed to provide a limited level of assurance and relies on the integrity of the host, it offers no security if the server is compromised or not used.

ACL design is complex - operators will not normally need to write ACLs themselves. Thales provide tools to generate keys with strong ACLs.

## Object re-use

All objects stored in the module are referred to by a handle. The module's memory management functions ensure that a specific memory location can only be allocated to a single handle. The handle also identifies the object type, and all of the modules enforce strict type checking. When a handle is released the memory allocated to it is actively zeroed.

## Error conditions

If the module cannot complete a command due to a temporary condition, the module returns a command block with no data and with the status word set to the appropriate value. The operator can resubmit the command at a later time. The server program can record a log of all such failures.

If the module encounters an unrecoverable error it enters the error state. This is indicated by the status LED flashing in the Morse pattern SOS. As soon as the unit enters the error state all processors stop processing commands and no further replies are returned. In the error state the unit does not respond to commands. The unit must be reset.

## Security Boundary

The physical security boundary is the plastic jig that contains the potting on both sides of the PCB.

All cryptographic components are covered by potting.

There is also a logical security boundary between the nCore kernel and the SEE.

Some items are excluded from FIPS 140-2 validation as they are not security relevant see Excluded Components on page 13.

## Status information

The module has a status LED that indicates the overall state of the module.

The module also returns a status message in the reply to every command. This indicates the status of that command.

There are a number of services that report status information.

Where the module is fitted inside an NetHSM this information can be displayed on the LCD on the NetHSM's front panel.

## Procedures to initialise a module to comply with FIPS 140-2 Level 2

The nShield enabled application must perform the following services, for more information refer to the nShield User Guide.

- 1 Put the mode switch into the initialisation position and restart the module
- 2 Use either the graphical user interface KeySafe or the command line tool **new-world**. Using either tool you must specify the number of cards in the Administrator Card Set and the encryption algorithm to use, Triple-DES or AES. To ensure that the module is in Level 2 mode you must
  - Using Keysafe select the option “**Strict FIPS 140 Mode**” = **No**
  - Using **new-world** do NOT specify the **-F** flag in the command line
- 3 The tool prompts you to insert cards and to enter a pass phrase for each card.
- 4 When you have created all the cards, reset the mode switch into the operational position and restart the module.

### Verifying the module is in level 2 mode

An operator can verify the initialisation status of the module as if a module is initialised in level 2 mode:

- Keysafe displays "Strict FIPS 140-2 Mode" = No in the information panel for that module.
- The command line tool Enquiry does NOT include **StrictFIPS** in the list of flags for the module



## Operating a level 2 module in FIPS mode

To be operating in Level 2 FIPS Mode, only FIPS Approved cryptography can be used in FIPS Mode. Use of any Non-FIPS Approved algorithms, except for those for which the CMVP allowed in FIPS Mode (See Supported Algorithms Section), means that the module would not be operating in FIPS Mode.

In order to comply with FIPS mode the operator must not generate private or secret keys with the **ExportAsPlain** ACL entry; nor should they use the **Import** service to import such keys in plain text.

An operator can verify that a key was generated correctly using the **nfmverify** utility supplied by Thales. This utility checks the ACL stored in the key-generation certificate.

## To return a module to factory state

1. Put the mode switch into the initialisation position. Pull the Initialisation pin high and restart the module.
2. Use the **Initialise** command to enter the Initialisation state.
3. Load a random value to use as the hash of the nCipher Security Officer's key.
4. Set nCipher Security Officer service to set the nCipher Security Officer's key and the operational policy of the module.
5. Put the mode switch into the operational position Pull the Initialisation pin low and restart the module.
6. After this operation the module must be initialized correctly before it can be used in a FIPS approved mode.

Placing the module in factory state:

- destroys any loaded Logical tokens, Share Keys, Impath keys, Key objects, Session keys
- erases the current Module Signing Key and generates a fresh one.
- erases all current Module Keys, except the Well Known Module Key
- Generates a new Module Key Zero
- sets nCipher Security Officer's key to a known value
- this prevent the module from loading any keys stored a key blobs as it no longer possesses the decryption key.

Returning the module to factory state does not erase the Firmware Confidentiality Key, the Long Term Signing Key or the public halves of the Firmware Integrity Key, of the Master Feature Enable Key: as these provide the cryptographic identity of the module and control loading firmware.

Thales supply a graphical user interface KeySafe and a command line tool **new-world** that automate these steps.

## To create a new operator

- 1 Create a logical token.
- 2 Write one or more shares of this token onto software tokens.
- 3 For each key the operator will require, export the key as a key blob under this token.
- 4 Give the operator any pass phrases used and the key blob.

Thales supply a graphical user interface KeySafe and a command line tool **new-world** that automate these steps.

## To authorize the operator to create keys

- 1 Create a new key, with an ACL that only permits **UseAsSigningKey**.
- 2 Export this key as a key blob under the operator's token.
- 3 Create a certificate signed by the nCipher Security Officer's key that:
  - includes the hash of this key as the certifier
  - authorizes the action **GenerateKey** or **GenerateKeyPair** depending on the type of key required.
- 4 if the operator needs to create permanent - as opposed to session - keys, the certificate must also include an entry that enables the action **MakeBlob**. The certificate can restrict the operator to only making blobs protected by their Operator Card Set by including the hash of its logical token.
- 5 Give the operator the key blob and certificate.

Thales supply a graphical user interface KeySafe and a command line tool **new-world** that automate these steps.

## To authorize an operator to act as a Junior Security Officer

- 1 Generate a logical token to use to protect the Junior Security Officer's key.
- 2 Write one or more shares of this token onto software tokens
- 3 Create a new key pair,
- 4 Give the private half an ACL that permits **Sign** and **UseAsSigningKey**.
- 5 Give the public half an ACL that permits **ExportAsPlainText**
- 6 Export the private half of the Junior Security Officer's key as a key blob under this token.
- 7 Export the public half of the Junior Security Officer's key as plain text.
- 8 Create a certificate signed by the nCipher Security Officer's key includes the hash of this key as the certifier
  - authorizes the actions **GenerateKey**, **GenerateKeyPair**
  - authorizes the actions **GenerateLogicalToken**, **WriteShare** and **MakeBlob**, these may be limited to a particular module key.
- 9 Give the Junior Security Officer the software token, any pass phrases used, the key blob and certificate.

Thales supply a graphical user interface KeySafe and a command line tool **new-world** that automate these steps.

## To authenticate an operator to use a stored key

- 1 Use the **LoadLogicalToken** service to create the space for a logical token.
- 2 Use the **ReadShare** service to read each share from the software token.
- 3 Use the **LoadBlob** service to load the key from the key blob.

The operator can now perform the services specified in the ACL for this key.

To assume nCipher Security Officer role load the nCipher Security Officer's key using this procedure. The nCipher Security Officer's key can then be used in certificates authorising further operations.

Thales supply a graphical user interface KeySafe and a command line tool **new-world** that automate these steps.

## To authenticate an operator to create a new key

- 1 If you have not already loaded your operator token, load it as above.
- 2 Use the **LoadBlob** service to load the authorization key from the key blob.
- 3 Use the **KeyId** returned to build a signing key certificate.
- 4 Present this certificate with the certificate supplied by the nCipher Security Officer with the **GenerateKey**, **GenerateKeyPair** or **MakeBlob** command.

Thales supply a graphical user interface KeySafe and a command line tool **new-world** that automate these steps.

## Chapter 9: Physical security

All security critical components of the module are covered by epoxy resin.

The module has a clear button. Pressing this button put the module into the self-test state, clearing all stored key objects, logical tokens and impath keys and running all self-tests. The long term security critical parameters, module keys, module signing key and nCipher Security Officer's key can be cleared by returning the module to the factory state, as described above.

### Checking the module

To ensure physical security, make the following checks regularly:

- Examine the epoxy resin security coating for obvious signs of damage.
- The smart card reader is directly plugged into the module or into a port provided by any appliance in which the module is integrated and the cable has not been tampered with. Where the module is in an appliance the security of this connection may be protected by the seals or other tamper evidence provided by the appliance.



# Chapter 10: Strength of functions

## Attacking Object IDs

Connections are identified by a **ClientID**, a random 32 bit number.

Objects are identified by an **ObjectID**, again this is a random 32 bit number.

In order to randomly gain access to a key loaded by another operator you would need to guess two random 32 bit numbers. There are  $2^{64}$  possibilities therefore meets the 1 in a  $10^6$  requirement.

The module can process about  $2^{16}$  commands per minute - therefore the chance of succeeding within a minute is  $2^{16} / 2^{64} = 2^{-48}$  which is significantly less than the required chance of 1 in  $10^5$  ( $\sim 2^{-17}$ ).

## Attacking Tokens

If an operator chooses to use a logical token with only one share, no pass phrase and leaves the smart card containing the share in the slot than another operator could load the logical token. The module does not have any idea as to which operator inserted the smart card. This can be prevented by:

- not leaving the smart card in the reader

if the smart card is not in the reader, they can only access the logical token by correctly guessing the **ClientID** and **ObjectID** for the token.

- requiring a pass phrase

when loading a share requiring a pass phrase the operator must supply the SHA-1 hash of the pass phrase. The hash is combined with a module key, share number and smart card id to recreate the key used to encrypt the share. If the attacker has no knowledge of the pass phrase they would need to make  $2^{80}$  attempts to load the share. The module enforces a five seconds delay between failed attempts to load a share.

- requiring more than one share

If a logical token requires shares from more than one smart card the attacker would have to repeat the attack for each share required.

Logical tokens are either 168-bit Triple DES keys or 256-bit AES keys. Shares are encrypted under a combination of a module key, share number and card ID. If you could construct a logical token share of the correct form without knowledge of the module key and the exact mechanism used to derive the share key the chance that it would randomly decrypt into a valid token are  $2^{-168}$  or  $2^{-256}$ .

## Key Blobs

Key blobs are used to protect keys outside the module. There are two formats of blob - indirect and direct.

If the module is configured with AES module key, the blobs used for token and module key protected keys take a 256 bit AES key and a nonce and uses SHA-1 to derive a AES encryption key, used for encryption and a HMAC SHA-1 key, used for integrity.

If the module is configured with Triple DES module key, the blobs used for token and module key protected keys use Triple DES and SHA-1 for encryption and integrity.

If the module is initialised in a fresh security world, the blobs used for key-recovery and for pass-phrase recovery take the public half of a 3072-bit RSA key and a nonce as the input, and uses SHA-256 to derive a 256-bit AES encryption key, used for encryption and a HMAC SHA-256 key, used for integrity.

If the module is enrolled into an old security world created before the release of 2.50.16 firmware, the blobs used for key-recovery and for pass-phrase recovery take the public half of a 1024-bit RSA key and a nonce as the input, and uses SHA-1 to derive a 168-bit triple-DES or 256-bit AES encryption key - depending on the option selected for the module key - and a HMAC SHA-1 key, used for integrity.

The firmware also supports key blobs based on an integrated encryption scheme using Diffie Hellman to establish a master secret and HMAC SHA-256 for integrity and AES in CBC mode for encryption, or HMAC SHA-1 for integrity and Triple DES in CBC mode for encryption. However, this option is currently not used by any Thales tools.

All schemes used in SP800-131 compliant security worlds offer at least 128-bits of security. Those used in legacy security worlds offer at least 80-bits of security.

## Impaths

Impaths protect the transfer of encrypted shares between modules.

When negotiating an Impath, provided both modules are configured to be SP800-131 compliant the module verifies a 3072-bit DSA signatures with SHA-256 hashes to verify the identity of the other module. It then uses 3072-bit Diffie-Hellman key exchange to negotiate a 256-bit AES encryption and MAC keys used to protect the channel. This provides a minimum of 128-bits of security for the encrypted channel.

Otherwise, both modules use 1024-bit DSA signatures to verify the identity of the other module. Then they perform a 1024-bit Diffie-Hellman key exchange to negotiate a 168-bit triple-DES encryption keys used to protect the channel. This provides a minimum of 80-bits of security for the encrypted channel.

**Note** The shares sent over the channel are still encrypted using their share key, decryption only takes place on the receiving module.

## KDP key provisioning

The KDP protocol used to transfer keys from a module to a micro HSM uses 1024-bit DSA signatures to identify the end point and a 2048-bit Diffie-Hellman key exchange to negotiate the Triple-DES or AES keys used to encrypt the keys in transit providing a minimum of 100-bits of security for the encrypted channel.

## Derived Keys

The nCore API provides a range of key derivation and wrapping options that an operator can choose to make use of in their protocols.

For any key, these mechanisms are only available if the operator explicitly enabled them in the key's ACL when they generated or imported the key.

The ACL can specify not only the mechanism to use but also the specific keys that may be used if these are known.

| Mechanism        | Use  | Notes                                     |
|------------------|--|---|
| Key Splitting    | Splits a symmetric key into separate components for split knowledge key export | Components are raw byte blocks.           |
| PKCS8 wrapping   | Encrypts a key using a pass phrase.  | Only available in FIPS 140-2 level 2 mode |
| PKCS8 unwrapping | Decrypts a wrapped key using a pass phrase.                                    | Only available in FIPS 140-2 level 2 mode |

| Mechanism                  | Use   | Notes  |
|----------------------------|---|--|
| SSL3 master key derivation | Setting up a SSL session  | Only available in FIPS 140-2 level 2 mode  |
| TLS master key derivation  | Setting up a TLS session  |  |
| Key Wrapping               | Encrypts one key object with another to allow the wrapped key to be exported. | May use any supported encryption mechanism that accepts a byteblock. The operator must ensure that they chose a wrapping key that has an equivalent strength to the key being transported. |

If the module is initialized in its level 3 mode you can only use key wrapping and key establishment mechanisms that use approved algorithms.

If the module is initialized in its level 2 mode you can only use key wrapping and key establishment mechanisms with all supported algorithms.

# Chapter 11: Self Tests

When power is applied to the module it enters the self test state. The module also enters the self test state whenever the unit is reset, by pressing the clear button.

In the self test state the module clears the main RAM, thus ensuring any loaded keys or authorization information is removed and then performs its self test sequence, which includes:

- An operational test on hardware components
- An integrity check on the firmware, verification of a SHA-1 hash.
- A statistical check on the random number generator
- Known answer and pair-wise consistency checks on all approved and allowed algorithms in all approved modes and of the DRBG
- Verification of a MAC on EEPROM contents to ensure it is correctly initialized.

This sequence takes a few seconds after which the module enters the Pre-Maintenance, Pre-Initialisation, Uninitialised or Operational state; depending on the position of the mode switch and the validity of the EEPROM contents.

While it is powered on, the module continuously monitors the temperature recorded by its internal temperature sensor. If the temperature is outside the operational range it enters the error state.

The module also continuously monitors the hardware entropy source and the approved AES-256 based DRBG. If either fail it enters the error state.

When firmware is updated, the module verifies a DSA signature on the new firmware image before it is written to flash.

In the error state, the module's LED repeatedly flashes the Morse pattern SOS, followed by a status code indicating the error. All other inputs and outputs are disabled.

## Firmware Load Test

When an administrator loads new firmware, the module reads the candidate image into working memory. It then performs the following tests on the image before it replaces the current application:

- The image contains a valid signature which the module can verify using the Firmware Integrity Key
- The image is encrypted with the Firmware Confidentiality Key stored in the module.
- The Version Security Number for the image is at least as high as the stored value.

Only if all three tests pass is the new firmware written to permanent storage.

Updating the firmware clears the nCipher Security Officer's key and all stored module keys. The module will not re-enter operational mode until the administrator has correctly re-initialized it.

# Chapter 12: Supported Algorithms

## FIPS approved and allowed algorithms:

### Symmetric Encryption

- AES  
Certificate #1579 (all other services)  
ECB, CBC GCM and CMAC modes
- Triple-DES  
#132 CBC mode (Channel Open and Channel Update Services only - these are offloaded to the Broadcom processor)  
Certificate #1035 (all other services)  
ECB and CBC mode

### Hashing and Message Authentication

- AES CMAC  
AES Certificate #1579
- AES GMAC  
AES Certificate #1579
- HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384 and HMAC SHA-512  
Certificate #925
- SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512  
Certificate #1398
- Triple-DES MAC  
Triple-DES Certificate #1035 vendor affirmed

## Signature

- DSA  
Certificate #487  
FIPS 186-2 and FIPS 186-3 signature generation and verification  
Modulus 1024-bits Sub-group 160-bits SHA-1  
Modulus 2048-bits Sub-group 224-bits SHA-224  
Modulus 2048-bits Sub-group 256-bits SHA-256  
Modulus 3072-bits Sub-group 256-bits SHA-256
- ECDSA  
Certificate #192  
FIPS 186-2: Signature Generation and Verification  
P-192 P-224 P-256 P-384 P-521 K-163 K-233 K-283 K-409 K-571 B-163 B-233 B-283  
B-409 and B-571 Curves
- RSA  
Firmware 2.50.16, 2.50.35: Certificate #770; Firmware 2.51.10, 2.55.1: Certificate #1092  
FIPS 186-2: RSASSA-PKCS1\_V1\_5 signature generation and verification  
FIPS 186-3: Key generation; RSASSA-PKCS1\_V1\_5 and RSASSA-PSS signature  
generation and verification

## Key Establishment

- Diffie-Hellman  
(CVL Cert. #1, key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength)
- Elliptic Curve Diffie-Hellman  
(CVL Cert. #1, key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength)
- EC-MQV  
(key establishment methodology provides between 80 and 256 of encryption strength)
- RSA  
(key wrapping, key establishment methodology provides between 80 and 256 bits of encryption strength)
- AES  
(AES Certificate #1579, key wrapping; key establishment methodology provides between



128 and 256 bits of encryption strength)

AES Key Wrap, AES CMAC Counter mode according to SP800-108, AES CBC mode

- Triple DES  
(Triple DES Certificate #1035, key wrapping; key establishment methodology provides 80 or 112 bits of encryption strength)  
CBC mode

## Other

- Deterministic Random Bit Generator  
Certificate #72  
SP 800-90 using Counter mode of AES-256

## Non-FIPS approved algorithms

Note Algorithms marked with an asterisk are not approved by NIST. If the module is initialised in its level 3 mode, these algorithms are disabled. If module is initialized in level 2 mode, the algorithms are available. However, if you choose to use them, the module is not operating in FIPS approved mode.

### Symmetric

- Aria\*
- Arc Four (compatible with RC4)\*
- Camellia\*
- CAST 6 (RFC2612)\*
- DES\*
- SEED (Korean Data Encryption Standard) - requires Feature Enable activation\*

### Asymmetric

- El Gamal\* (encryption using Diffie-Hellman keys)
- KCDSA (Korean Certificate-based Digital Signature Algorithm) - requires Feature Enable activation\*
- RSA encryption and decryption\*

### Hashing and Message Authentication

- HAS-160 - requires Feature Enable activation\*
- MD5 - requires Feature Enable activation\*
- RIPEMD 160\*
- Tiger\*
- HMAC (MD5, RIPEMD160, Tiger)\*

## Non-deterministic entropy source

Non-deterministic entropy source, used to seed approved random bit generator.

## Other

- SSL\*/TLS master key derivation
- PKCS #8 padding\* .

Note TLS key derivation is approved for use by FIPS 140-2 validated modules - though there is as yet no validation test. MD5 may be used within TLS key derivation.

# Contact Us

Web site: <https://www.ncipher.com>  
Help Centre: <https://help.ncipher.com>  
Email Support: [support@ncipher.com](mailto:support@ncipher.com)  
Contact Support Numbers: <https://www.ncipher.com/services/support/contact-support>

## About nCipher Security

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business critical information and applications. Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensure the integrity of your data and put you in complete control – today, tomorrow, always. [www.ncipher.com](http://www.ncipher.com)

Search: nCipherSecurity



TRUST. INTEGRITY. CONTROL.