



Thales nShield HSM Security Policy

nShield F2 10e, nShield F2 500e, nShield F2 1500e, nShield F2 6000e in FIPS 140-2 level 2 mode

Version: 4.6

Date: 03 May 2016

Copyright 2015 Thales UK Limited and Thales e-Security. All rights reserved.

This document is non-proprietary. Reproduction is authorised provided the document is copied in its entirety without modification and including this copyright notice.

Information in this document is subject to change without notice.

Thales UK Limited and Thales e-Security make 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. Thales UK Limited and Thales e-Security shall not be liable for errors contained herein or for incidental or consequential damages concerned with the furnishing, performance or use of this material.

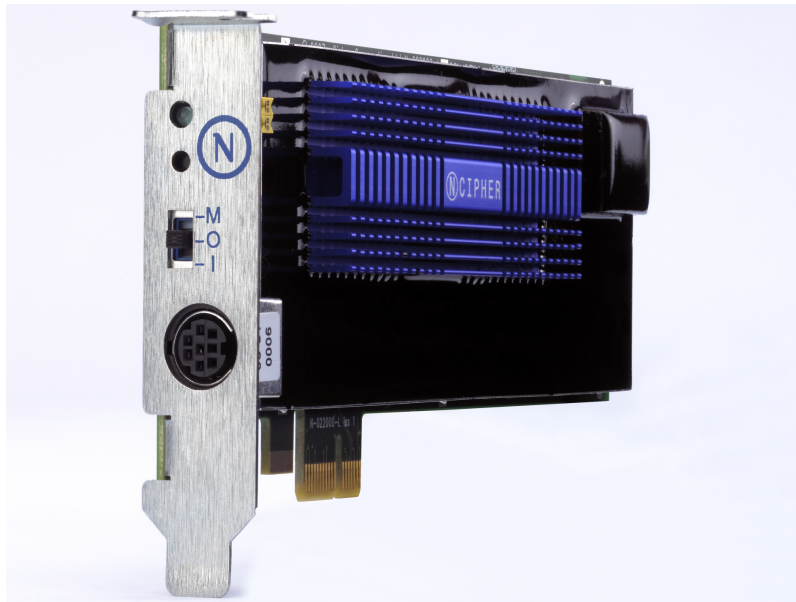
Contents

Contents	3
Chapter 1: Purpose	4
Chapter 2: Ports and Interfaces	6
Chapter 3: Roles	7
Chapter 4: Services available to each role	9
Chapter 5: Keys	27
Chapter 6: Rules	34
6.1 Identification and authentication	34
6.2 Procedures to initialize a module to comply with FIPS 140-2 Level 2	36
6.3 Operating a level 2 module in FIPS mode	37
6.4 To return a module to factory state	37
6.5 To create a new operator	38
6.6 To authorize the operator to create keys	38
6.7 To authorize an operator to act as a Junior Security Officer	38
6.8 To authenticate an operator to use a stored key	39
6.9 To authenticate an operator to create a new key	39
Chapter 7: Physical security	40
Chapter 8: Strength of functions	41
Chapter 9: Self Tests	45
9.1 Firmware Load Test	45
Chapter 10: Supported Algorithms	46
10.1 FIPS approved and allowed algorithms:	46
10.2 Non-FIPS approved algorithms	49
Addresses	50

Chapter 1: Purpose

Thales nShield tamper evident and tamper responsive Hardware Security Modules provide support for the widest range of cryptographic algorithms, application programming interfaces (APIs) and host operating systems, enabling the devices to be used with virtually any business application—from identity management, web services and database encryption to tokenization, PKI services and strong authentication.

The following figure shows the Thales nShield cryptographic module:



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

Unit ID	Model Number	Real Time Clock (RTC) NVRAM	Secure Execution Environment (SEE)	Potting (epoxy resin)	EMC classification	Crypto Accelerator	Overall FIPS level
nShield F2 6000e	nC3023E-6K0	Yes	No	Yes	A	Yes	2
nShield F2 1500e	nC3023E-1K5	Yes	No	Yes	A	Yes	2
nShield F2 500e	nC3023E-500	Yes	No	Yes	A	Yes	2
nShield F2 10e	nC3023E-010	Yes	No	Yes	A	None	2

The units are identical in appearance and operation and only vary in the processing speed.

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

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

The modules run 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 **New Enquiry** service which reports the version of firmware currently loaded. The validated firmware version is 2.61.2-2.

The module can be initialized to comply with the requirements for Roles and Services at either level 2 or level 3.

The initialization parameters are reported by the **New Enquiry** and **Sign Module State** 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.

The 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 an on-board Real-time clock.

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

- Windows
- Solaris
- HP-UX
- AIX
- Linux x86 / x64

Windows was used to test the module for this validation.

Section	Level
1. Cryptographic Module Specification	2
2. Cryptographic Module Ports and Interfaces	2
3. Roles, Services, and Authentication	3
4. Finite State Model	2
5. Physical Security	3
6. Operational Environment	N/A
7. Cryptographic Key Management	2
8. EMI/EMC	3
9. Self-Tests	2
10. Design Assurance	3
11. Mitigation of Other Attacks	N/A
Overall FIPS Level	2

Chapter 2: Ports and Interfaces

The module has the following physical ports:

- PCIe bus (data input/output, control input, status output and power). The services provided by the module are transported through this interface.
- Status LED (status output)
- Mode switch (control input)
- Clear button (control input)
- PS/2 serial connector and 14-pin header (data input/output) for connecting a smartcard reader.

The actual physical connectors are outside the cryptographic boundary and the PCB traces coming from those connectors transport the signals into the module's cryptographic boundary.

Chapter 3: Roles

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

Unauthenticated

All connections are initially unauthenticated.

An operator in the unauthenticated role does not have access to handles or tickets required to provide access to the CSPs of authenticated users.

User

An operator assumes 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.

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 an nShield Security Officer authorizing the action. Some actions including writing tokens always require a certificate.

nShield Security Officer

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

The nShield 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 nShield 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 **ObjectID** for this key to authorize a command.

Junior Security Officer

Where the nShield 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 **ObjectID** 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 4: Services available to each role

This section describes all the services supported by the module. The functions available depend on whether the operator has assumed the unauthenticated role, the user or junior security officer (JSO) roles, or the nShield Security Officer (NSO) role. The reader can refer to the Terminology table at the end of this section for an explanation of the terms used. 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.

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	

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
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.	Sets 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	handle, ACL	handle, ACL	handle, ACL	Opens a communication channel which can be used for bulk encryption, decryption, signing or hashing.	Uses a key object	AES, Triple DES, DES*, Arc Four*, Aria*, Camellia*, SEED*, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 RSA, DSA, ECDSA, Triple DES MAC, HMAC, KCDSA*

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
Channel Update	handle	handle	handle	Performs encryption, decryption, signing or hashing on a previously opened channel. The operation and key are specified in ChannelOpen .	Uses a key object	AES, Triple DES, DES [*] , Arc Four [*] , Aria [*] , Camellia [*] , SEED [*] , SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 RSA, DSA, ECDSA, Triple DES MAC, HMAC, KCDSA [*]
Clear Unit	Yes	Yes	Yes	Causes the module to reset and will trigger the Self-tests. Zeroizes all loaded keys, tokens and shares. Clear Unit does not erase long term keys, such as module keys.	Zeroizes objects.	All
Create Buffer	No	cert	Yes	Allocates an area of memory to load data. If the data is encrypted, this service specifies the encryption key and IV used. The decrypt operation is performed by LoadBuffer	Uses a key object	AES, Triple DES, DES [*] , Arc Four [*] , Aria [*] , Camellia [*] , SEED [*]
Decrypt	handle, ACL	handle, ACL	handle, ACL	Decrypts a cipher text with a stored key returning the plain text.	Uses a key object	AES, Triple DES, DES [*] , Arc Four [*] , Aria [*] , Camellia [*] , SEED [*] , RSA [*] , ElGamal [*] , KCDSA [*]

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
Derive Key	handle, ACL	handle, ACL	handle, ACL	The DeriveKey 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.	Uses a key object, create a new key object.	AES, AES key wrap, RSA, EC-DH, EC-MQV, Triple DES, PKCS #8*, TLS key derivation*, XOR, DLIES (D/H plus Triple DES or D/H plus AES), Aria*, Arc Four*, Camellia*, DES*, SEED*
Destroy	handle	handle	handle	Removes an object, if an object has multiple handles as a result of RedeemTicket service, this removes the current handle.	Erases a impath, logical token, or any key object.	All
Duplicate	handle, ACL	handle, ACL	handle, ACL	Creates a second instance of a key object with the same ACL and returns a handle to the new instance.	Creates a new key object.	All
Dynamic Slot Create Association	Yes	Yes	Yes	Creates a slot association used to reserve and identify a dynamic slot for use by this client.	No access to keys or CSPs	
Dynamic Slot Exchange APDUs	No	handle	handle	Exchange Application Protocol Data Units with the remote Javacard.	Uses secure channel integrity and confidentiality keys	[AES, AES-CMAC, ECDH, ECDSA]
Dynamic Slots Configure	Yes	Yes	Yes	Instructs a module to reconfigure itself to have the given number of dynamic smartcard slots.	No access to keys or CSPs	

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
Dynamic Slots Configure Query	Yes	Yes	Yes	Queries a module to determine whether it has had its dynamic slots configured.	No access to keys or CSPs	
Encrypt	handle, ACL	handle, ACL	handle, ACL	Encrypts a plain text with a stored key returning the cipher text.	Uses a key object	AES, Triple DES, RSA*, DES, ElGamal*, Arc Four*, Aria*, Camellia*, SEED*, KCDSA*
Erase File	Yes	Yes	Yes	Removes a file, but not a logical token, from a smart card or software token.	No access to keys or CSPs	
Erase Share	Yes	Yes	Yes	Removes a share from a smart card or software token.	Erases a share	
Export	handle, ACL	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 37 .	Exports a [public] key object.	Any key type
Fail	Yes	Yes	Yes	Causes the module to enter a failure state.	No access to keys or CSPs	
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]
File Copy	No	cert, ACL	ACL	Copies a file. You can only copy files in their entirety. Requires file copying permission, and permission to create the file on the target device.	No access to keys or CSPs	

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
File Create	No	cert	Yes	Creates a file on the given device. The file is created with the size given in the file argument, and is initially filled with zeroes. The file must not exist. This prevents overwriting and race conditions.	No access to keys or CSPs	
File Op	No	cert, ACL	ACL	Does an operation on a file, e.g. read, write, delete. Requires that the file's ACL permit the operation.	No access to keys or CSPs	
Firmware Authenticate	Yes	Yes	Yes	Reports firmware version. Performs a zero knowledge challenge response protocol based on HMAC that enables a 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	No	handle	handle	Sends an ISO-7816 command to a smart card over the channel opened by ForeignTokenOpen .	No access to keys or CSPs	
Foreign Token Open	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 FormatToken . The channel is closed when the card is removed from the reader, or if the handle is destroyed. This service is feature enabled.	No access to keys or CSPs	

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
Format Token	Yes	Yes	Yes	Formats a smart card or software token ready for use.	May use a module key to create challenge response value	[AES, Triple DES]
Generate Key	Yes	Yes	Yes	Generates a symmetric key of a given type with a specified ACL and returns a handle. Optionally returns a certificate containing the ACL. The data generated by this operation is not a CSP until it has been bound to an authorized user by protecting it with a token.	Creates a new symmetric key object. Sets the ACL and Application data for that object. Optionally uses module signing key and exports the key generation certificate.	AES, Triple DES, Arc Four*, Aria*, Camellia*, DES*, SEED*
Generate Key Pair	Yes	Yes	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. The data generated by this operation is not a CSP until it has been bound to an authorized user by protecting it with a token.	Creates two new key objects. Sets the ACL and Application data for those objects. Optionally uses module signing key and exports two key generation certificates.	Diffie-Hellman, DSA, ECDSA, EC-DH, EC-MQV, RSA, ElGamal*, KCDSA*
Generate Logical Token	Yes	Yes	Yes	Creates a new logical token, which can then be written as shares to smart cards or software tokens. On creation the token is not a CSP as it does not protect any sensitive data.	Uses module key. Creates a logical token.	[AES or Triple DES]
Get ACL	handle, ACL	handle, ACL	handle, ACL	Returns the ACL for a given handle.	Exports the ACL for a key object.	

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
Get Application Data	handle, ACL	handle, ACL	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	handle	handle	handle	Superseded by GetKeyInfoExtended , retained for compatibility.	<i>Exports</i> the SHA-1 hash of a key object	
Get Key Info Extended	handle	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 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 Logical Token Info	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 nShield 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.	[DSA]
Get Module State	Yes	Yes	Yes	Returns unsigned data about the current state of the module.	No access to keys or CSPs	
Get RTC	Yes	Yes	Yes	Reports the time according to the on-board real-time clock	No access to keys or CSPs	

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
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.	
Get Slot Info	Yes	Yes	Yes	Reports status of the physical token in a slot. Enables an operator to determine if the correct token is present before issuing a ReadShare command. If the token was formatted with a challenge response value, uses the module key to authenticate the smart card.	<i>Uses</i> a module key if token is formatted with a challenge response value.	[AES, Triple DES]
Get Slot List	Yes	Yes	Yes	Reports the list of slots available from this module.	No access to keys or CSPs	
Get Ticket	handle	handle	handle	Gets a ticket - an invariant identifier - for a key. This can be passed to another client which can redeem it using RedeemTicket to obtain a new handle to the object,	<i>Uses</i> a key object, logical token, impath.	
Hash	Yes	Yes	Yes	Hashes a value.	No access to keys or CSPs	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
Impath Get Info	No	handle	handle	Reports status information about an impath	<i>Uses</i> an Impath, <i>exports</i> status information.	
Impath Key Exchange Begin	FE	FE	FE	Creates a new inter-module path and returns the key exchange parameters to send to the peer module.	<i>Creates</i> a set of Impath keys	[DSA and Diffie Hellman] AES, Triple-DES
Impath Key Exchange Finish	No	handle	handle	Completes an impath key exchange. Require the key exchange parameters from the remote module.	<i>Creates</i> a set of Impath keys.	[DSA and Diffie Hellman, AES, Triple DES]

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
Impath Receive	No	handle	handle	Decrypts data with the Impath decryption key.	Uses an Impath key.	[AES or Triple DES]
Impath Send	No	handle	handle	Encrypts data with the impath encryption key.	Uses an Impath key.	[AES or Triple DES]
Import	Yes	Yes	Yes	Loads a key and ACL from the host and returns a handle. The data generated by this operation is not a CSP until it has been bound to an authorized user by protecting it with a token. 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 37	Creates a new key object to store imported key, sets the key value, ACL and App data.	
Initialise Unit	init	init	init	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. This can only be performed when the module is in initialization mode. It also generates a new KM0 and module signing key. 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.	Erases all keys, Creates KM0 and KML	[DSA]

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
Insert Soft Token	Yes	Yes	Yes	Allocates memory on the module that is used to store one or more logical shares or other Token data objects.	No access to keys or CSPs	
Load Blob	No	handle	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.	<i>Uses</i> module key, logical token, or archiving key, <i>creates</i> a new key object.	Triple DES and SHA-1 or AES, DH, or RSA plus AES, SHA-1, and HMAC SHA-256 (256 bit key) or HMAC SHA-1 (160 bit key)
Load Buffer	No	handle	handle	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. Requires the handle of a buffer created by CreateBuffer .	No access to keys or CSPs	
Load Logical Token	yes	yes	yes	Allocates space for a new logical token - the individual shares can then be assembled using ReadShare or ReceiveShare . Once assembled the token can be used in LoadBlob or MakeBlob commands.	<i>Uses</i> module key	[AES or Triple DES]

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
Make Blob	No	handle, ACL	handle, ACL	Creates a key blob containing the key and returns it. The key object to be exported may be any algorithm.	Uses module key, logical token or archiving key, exports encrypted key object.	Triple DES and SHA-1 or AES, DH, or RSA plus AES, SHA-1, and HMAC SHA-256 (256 bit key) or HMAC SHA-1 (160 bit key)
Mod Exp	Yes	Yes	Yes	Performs a modular exponentiation on values supplied with the command.	No access to keys or CSPs	
Mod Exp CRT	Yes	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	Yes	Reports low level status information about the module. This service is designed for use in Thales' test routines.	No access to keys or CSPs	
New Enquiry	Yes	Yes	Yes	Reports status information (Show Status).	No access to keys or CSPs	
No Operation	Yes	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	Yes	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	Yes	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	

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
NVMem List	Yes	Yes	Yes	Reports a list of files stored in the non-volatile memory or protected by an ACL on a smart card.	No access to keys or CSPs	
NVMem Operation	No	cert, ACL	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	
Random number	Yes	Yes	Yes	Generates a random number for use in a application using the on-board random number generator. There are separate services for generating keys. The random number services are designed to enable an application to access the random number source for its own purposes - for example an on-line casino may use GenerateRandom to drive its applications.	Uses DRBG key	[AES]
Random prime	Yes	Yes	Yes	Generates a random prime. This uses the same mechanism as is used for RSA and Diffie-Hellman key generation. The primality checking conforms to ANSI X9.31.	Uses DRBG key	[AES]

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
Read File	Yes	Yes	Yes	Reads a file, but not a logical token, from a smart card or software token. This command can only read files without ACLs.	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 ReadShare or ReceiveShare commands.	Uses pass phrase, module key, creates share key, uses share key, creates a logical token.	[SHA-1, AES or Triple DES]
Receive Share	No	handle, encrypted share	handle, encrypted share	Takes a share encrypted with SendShare and a pass phrase and uses them to recreate the logical token. - may require several ReadShare or ReceiveShare commands	Uses an Impath key, uses pass phrase, module key, creates share key, uses share key, creates a logical token	[AES, Triple DES]
Redeem Ticket	ticket	ticket	ticket	Gets a handle in the current name space for the object referred to by a ticket created by GetTicket .	Uses a key object, logical token, impath	
Remove KM	No	cert	Yes	Removes a loaded module key.	Erases a module key	
Remove Soft Token	Yes	Yes	Yes	Removes a soft token. Copies the updated shares to the host and deletes them from the module's memory.	No access to keys or CSPs	

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
Secure Execution Environment (SEE) control	No	cert	cert	Support for SEE machines. SEE machines are outside the FIPS boundary.	No access to keys or CSPs	
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 ReceiveShare	Uses an impath key, exports encrypted share.	[AES, Triple DES]
Set ACL	handle, ACL	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	handle, ACL	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	Designates a key hash as the nShield 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 initialization state.	Sets the identity of the nShield Security officer's key.	[SHA-1 hash of DSA key]
Set RTC	No	cert	Yes	Sets the real-time clock.	No access to keys or CSPs	
Sign	handle, ACL	handle, ACL	handle, ACL	Returns the digital signature or MAC of plain text using a stored key.	Uses a key object	RSA, DSA, ECDSA, Triple DES MAC, HMAC, KCDSA*
Sign Module State	handle, ACL	handle, ACL	handle, ACL	Signs a certificate describing the modules security policy, as set by SetNSOPerm.	Uses the module signing key	[DSA]
Statistic Get Value	Yes	Yes	Yes	Reports a particular statistic.	No access to keys or CSPs	

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
Statistics Enumerate Tree	Yes	Yes	Yes	Reports the statistics available.	No access to keys or CSPs	
Update Firmware	monitor	monitor	monitor	<p>This service is used in the update firmware service.</p> <p>Thales supply the LoadROM utility for the administrator to use for this service. This utility issues the correct command sequence to load the new firmware. The module will only be operating in a FIPS approved mode if you install firmware that has been validated by NIST / CSE. Administrators who require FIPS validation should only upgrade firmware after NIST / CSE 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>	[DSA, AES]
Verify	handle, ACL	handle, ACL	handle, ACL	Verifies a digital signature using a stored key.	<i>Uses</i> a key object.	RSA, DSA, ECDSA, Triple DES MAC, HMAC, KCDSA*
Verify Certificate	Yes	Yes	Yes	Verifies a certificate. If the certificate (including any delegation chain) verifies correctly, then the command succeeds.	Access to keys?	[ECDSA public keys]
Write File	Yes	Yes	Yes	Writes a file, but not a logical token, to a smart card or software token. Note these files do not have an ACL, use the NVMEM commands to create files with an ACL.	No access to keys or CSPs	

Command / Service	Role			Description	Key/CSP access	Key types
	Unauth	JSO / User	NSO			
Write Share	No	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.</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.</p>
ACL	<p>Access Control List. 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 nShield Security Officer. This certificate will reference a key. The module verifies the signature on the certificate before permitting the operation.
FE	Feature Enable. This service is not available on all modules. It must be enabled using the FeatureEnable service before it can be used.
encrypted share	The ReceiveShare command requires a logical token share encrypted using an Impath key created by the SendShare command.
ticket	The RedeemTicket command requires the ticket generated by GetTicket .
init	These services are used to initialize the module. They are only available when the module is in the initialization mode. To put the module into initialization mode, either physically move the mode switch to the Initialization setting and use the Clear Unit command / service to clear the module, or invoke the Clear Unit command / service using a command line utility specifying Initialization as a parameter. In order to restore the module to operational mode you must put the mode 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 5: Keys

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

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

nShield Security Officer's key

The nShield Security officer's key must be set as part of the initialization process. This is a public / private key pair that the nShield 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 nShield Security Officer.

If you use the standard tools supplied by Thales to initialize 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 nShield 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 nShield 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 initialize 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.

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 nShield 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 or 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 logical token is exported the logical token - the key data 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 (which may require knowledge of a passphrase to derive - see Share keys) 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 keys

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 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 3072-bit Diffie-Hellman.

The Diffie Hellman operations has been validated in CVL Cert. #516. The CVL Cert. #516 is not fully compliant to SP 800-56A as the key derivation function has not been tested.

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. All impath keys are stored as objects in the object store in SRAM.

nShield Remote Administration Token Secure Channel

A Secure Channel is a secure channel between a Remote Administration token (Javacard) and a module.

To set up a secure channel two modules perform a key-exchange, using Elliptical Curve Diffie-Hellman with P-521 curves, to negotiate a 256-bit AES encryption and MAC keys used to protect the channel.

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 using an approved SP 800-108 Key Derivation Function.

Currently symmetric keys are AES-256. The four keys are used for encryption, decryption, MAC creation, MAC validation. The protocol ensures that the remote administration token key used for encryption is used for decryption by the module. All secure channel keys are stored as objects in the object store in SRAM.

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. An operator may pass a key reference to another operator 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 key encapsulation mechanism 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 key encapsulation mechanism 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 nShield 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 nShield 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' 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 devices in the nShield family of HSMs 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.

The Master Feature Enable Key is a DSA key pair. The private half of this key pair is stored at Thales' 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

DRBG stands for Deterministic Random Bit Generator.

The module uses the CTR_DRBG from SP 800-90A with a 256-bit AES key. This key is seeded from the on board entropy source whenever the module is initialized and is reseeded according to SP 800-90A with a further 1024 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.

The DRBG internal state is contained within the DRBG mechanism boundary and is not accessed by non-DRBG functions or by other instances of any DRBG.

Note: For CTR DRBG, the values of V and Key (SP 800-90A) are the 'secret values' of the internal state.

Chapter 6: Rules

6.1 Identification and authentication

Communication with the 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 server, 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 9](#). An operator cannot access any service that accesses CSPs without first presenting a smart card, or software token.

The nShield modules perform 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 nShield Security Officer, who is identified by a public key pair created when the module is initialized. It is not possible to change the nShield 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 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. Recorded error status codes may be queried without interaction with the module. 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.

Some components are excluded from FIPS 140-2 validation as they are not security relevant see [Ports and Interfaces on page 6](#).

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.

6.2 Procedures to initialize 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.

Put the module into initialization mode by calling the Initialise Unit command.

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 "**FIPS 140 Mode level 3 compliant**" = **No** ; or

Using **new-world** do NOT specify the **-F** flag in the command line

The tool prompts you to insert cards and to enter a pass phrase for each card.

When you have created all the cards, put the module back into operational mode as described in Chapter 4.

Verifying the module is in level 2 mode

An operator can verify that the module is operating in level 2 mode by verifying the following:

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

6.3 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.

6.4 To return a module to factory state

1. Put the mode switch into the initialization position Pull the Initialization pin high and restart the module.
2. Use the **Initialise** command to enter the Initialization state.
3. Load a random value to use as the hash of the nShield Security Officer's key.
4. Set nShield Security Officer service to set the nShield Security Officer's key and the operational policy of the module.
5. Put the mode switch into the operational position Pull the Initialization 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 nShield Security Officer's key to a known value
- this prevents 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.

6.5 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.

6.6 To authorize the operator to create keys

1. Create a new key, with an ACL that only permits **UseAsCertificate**.
2. Export this key as a key blob under the operator's token.
3. Create a certificate signed by the nShield Security Officer's key that:
 - includes the hash of this key as the certifier.
 - authorizes the action **OriginateKey** depending on the type of key required.
4. 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.

6.7 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 nShield 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.

6.8 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 nShield Security Officer role load the nShield Security Officer's key using this procedure. The nShield 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.

6.9 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 nShield 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 7: Physical security

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

The module hardness testing was only performed at a single temperature and no assurance is provided for Level 3 hardness conformance at any other temperature.

The module has a clear button. Pressing this button puts 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, nShield Security Officer's key, module keys and module signing 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 8: Strength of functions

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 ($\sim 2^{-17}$)

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 then 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 initialized 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. This mode of operation is non-approved.

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 SP 800-131A compliant security worlds offer at least 112-bits of security. Legacy security worlds, which offer at least 80-bits of security, operate in non-approved mode.

Impaths

Impaths protect the transfer of encrypted shares between modules.

When negotiating an Impath, provided both modules use 2.50.16 or later firmware, 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. The module will be operating in a non-approved mode when 1024-bit DSA signatures are used.

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

nShield Remote Administration Token Secure Channel

The Secure Channel protects the transfer of encrypted shares between a Remote Administration token and module.

When negotiating a Secure Channel the module verifies a ECDSA P-521 signature with SHA-512 hashes to verify the identity of the other module.

It then uses ECDH key exchange to negotiate 256-bit AES encryption and MAC keys used to protect the channel. This provides a minimum of 256-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 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
SSL/TLS master key derivation	Setting up an SSL/TLS session	Non-compliant. The protocols SSL, TLS shall not be used when operated in FIPS mode. In particular, none of the keys derived using this key derivation function can be used in the Approved mode.

Mechanism	Use	Notes
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. The operator must ensure that they chose a wrapping key that has an equivalent strength to the key being transported.
Secure Channel Key Derivation	Derivation of encryption and authentication keys for the secure channel	NIST SP 800-108 KDF

In level 2 mode you can use key wrapping and key establishment mechanisms with all supported algorithms.

Chapter 9: 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 or by sending the Clear Unit command.

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 checks as required by FIPS 140-2.
- 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-Initialization, Uninitialized or Operational state; depending on the position of the mode switch and the validity of the EEPROM contents.

The module also runs continuous random number generator tests on 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.

The module also performs pairwise-consistency checks when generating asymmetric key-pairs.

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.

9.1 Firmware Load Test

When new firmware is loaded, 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 nShield 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.

Note that if the module's firmware is updated to a different version, this results in the loss of the current CMVP validation of the module.

Chapter 10: Supported Algorithms

10.1 FIPS approved and allowed algorithms:

Symmetric Encryption

AES

Certificate #3420

ECB, CBC, GCM (externally generated IVs are non-compliant) and CMAC modes

Triple-DES

Certificate #1931

ECB and CBC modes (encryption with two-key Triple DES is non-compliant)

Hashing and Message Authentication

AES CMAC

AES Certificate #3420

AES GMAC

AES Certificate #3420

HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384 and HMAC SHA-512

Certificate #2178

SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512

Certificate #2826

Triple-DES MAC

Triple-DES Certificate #1931 vendor affirmed

(MAC generation with two-key Triple DES is non-compliant)

Signature

DSA

Certificate #964

FIPS 186-4: Signature generation and verification (Signature generation is non-compliant for SHA-1, and for keys less than 2,048 bits.)

Modulus 1024-bits, Sub-group 160-bits

Modules 2048-bits, Sub-group 224-bits

Modules 2048-bits, Sub-group 256-bits

Modules 3072-bits, Sub-group 256-bits

ECDSA

Certificate #695

FIPS 186-4: Signature generation and verification (Signature generation is non-compliant for SHA-1, and for values of n less than 224 bits, and for the curves P-192 K-163 and B-163.)

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

Certificate #1752

FIPS 186-4: Key generation; RSASSA PKCS1_V1_5 and RSASSA-PSS signature generation and verification (Signature generation with SHA-1 or keys sizes 1024 bits or 4096 bits is non-compliant.)

Modulus 1024 - 4096 bits with SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512

Key Establishment

Diffie-Hellman

Diffie-Hellman (CVL Cert. #516, key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

Elliptic Curve Diffie-Hellman

EC Diffie-Hellman (CVL Cert. #532, key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

RSA

RSA (key wrapping, key establishment methodology provides between 112 and 256 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

AES

KTS (Cert. #3446, key wrapping; key establishment methodology provides between 128 and 256 bits of encryption strength)

Triple-DES

Triple-DES (Cert. #1931, key wrapping; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

CBC mode (key wrapping with two-key Triple DES is non-compliant)

EC-MQV

ECMQV (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

Key Derivation

SP 800-108 Key Derivation #56 in Counter Mode.

Other**Deterministic Random Bit Generator**

Certificate #825

SP 800-90A using Counter mode of AES-256

10.2 Non-FIPS approved algorithms

Note: Algorithms marked with an asterisk are not approved by NIST. If used, the module will not be operating in the approved mode of operation.

Symmetric

- Aria^{*}
- Arc Four (compatible with RC4)^{*}
- Camellia^{*}
- CAST-256 (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^{*} (Same RSA implementation as used for key wrapping)

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 (non-compliant). The protocols SSL, TLS shall not be used when operated in FIPS mode. In particular, none of the keys derived using this key derivation function can be used in the Approved mode.

PKCS #8 padding^{*}.

Addresses

Americas

900 South Pine Island Road, Suite 710, Plantation, Florida 33324, USA

Tel: +1 888 744 4976 or + 1 954 888 6200

sales@thalessec.com

Europe, Middle East, Africa

Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ, UK

Tel: + 44 (0)1844 201800

emea.sales@thales-ecurity.com

Asia Pacific

Units 4101, 41/F. 248 Queen's Road East, Wanchai, Hong Kong, PRC

Tel: + 852 2815 8633

asia.sales@thales-ecurity.com

Internet addresses

Web site: <http://www.thales-ecurity.com/>
Support: <http://www.thales-ecurity.com/support-landing-page>
Online documentation: <http://www.thales-ecurity.com/knowledge-base>
International sales offices: <http://www.thales-ecurity.com/contact>