THALES

nShield Connect 6000, nShield Connect 1500 and nShield Connect 500

FIPS 140-2 Security Policy

www.thalesgroup.com/iss

Legal

Version: 0.3

Date: 30 November 2010

Patents

UK Patent GB9714757.3. Corresponding patents/applications in U

SA, Canada, South Africa, Japan and International Patent Application PCT/GB98/00142.

Versions

Version	Date	Author	Comments
0.1	2 May 2009	Marcus Streets	Initial Version
0.2	10 May 2009	Marcus Streets	Comments from Domus
0.3	30 November 2010	Marcus Streets	Comments from NIST

Chapter 1: Purpose

Thales nShield Connect is a network-attached hardware security module for business continuity of always-on, mission-critical systems in shared infrastructures.

The nShield Connect provides high availability, scalability and remote management for cryptographic infrastructures. Part of the nCipher product line, nShield Connect is the world's first Hardware Security Module (HSM) with redundant, hot-swappable power supplies.

The nShield Connect enables organizations to build reliable, large-scale cryptographic services for their infrastructures.

The nShield Connect is a 1U 19-inch rack mount appliance containing an nShield PCIe module running FIPS validated firmware, FIPS 140-2 Certificate 1063.

Unit ID	Model Number	Build Standard	Firmware Version
nShield Connect 6000	NH2047	N	V11.30
nShield Connect 1500	NH2040	N	V11.30
nShield Connect 500	NH2033	N	V11.30

The nShield Connect encrypts network traffic to provide trusted channels between operators running on remote servers and the nShield PCIe module within the nShield Connect.

Multiple operators may connect to the nShield Connect simultaneously. The nShield Connect establishes a separate set of keys for each connection, therefore each operator has its own trusted channel.

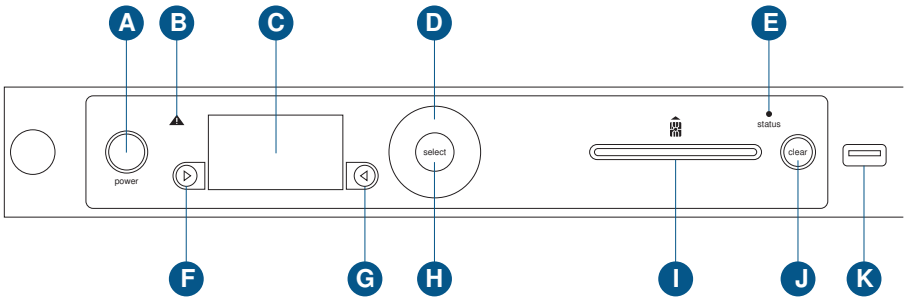
The nShield Connect is as multi-chip stand-alone cryptographic modules as defined by FIPS PUB 140-2.

The product meets the overall requirements applicable to Level 3 security for FIPS 140-2.

Security Requirements Section	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles and Services and Authentication	3
Finite State Machine Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	3
Overall Level of Certification	3

Chapter 2: Ports and Interfaces

Figure 1 Location of ports and interfaces on the nShield Connect front panel.



Physical ports

Ethernet ports

The module has two EJ-45 Ethernet ports on the rear panel. The ports are logically equivalent.

Power

The module has two field replaceable power supply units (PSUs) with standard IEC power connectors. The power supplies accept a wide range of input voltages 110V to 240V.

Power Switch

A front panel button (A) switches the enables an operator to switch the module in and out of stand-by mode. Turning the module on causes it to perform its self-tests.

USB

The module has a Universal Serial Bus (USB) interface (K) on the front panel that can accept keyboard input from an operator.

The interface is disabled when the module is in the standby and self test states.

Control buttons and wheel

There is a control wheel (D) and three buttons on the front panel that allow an operator to select menu options from the display. Unless the operator has authenticated as a Crypto-Officer, they can only select Show Status services.

Two buttons are placed under the display (F and G), the third (H) is in the centre of the control wheel.

The control wheel allows the operator in the Crypto-Officer role to change the selected menu item on the display.

Display

There is a half VGA Liquid Crystal Display (C) mounted on the front panel. This displays a menu system, which allows the operator in Crypto-Officer role to select commands. It can also display selected status information.

Warning LED

The orange warning Light Emitting Diode (LED) (B) is illuminated if the module has detected a problem that requires attention from an Crypto-Officer. This includes a tamper event, PSU or fan failure.

Smart Card Interface

There is a smart card reader (I) on the module front panel. This is used to authenticate Crypto-Officers.

Status LED

The blue status LED (E) displays the status of the nShield Connect.

Clear Button

A button on the front panel (J) enables an operator in Crypto-Officer role to reset the module, this clears all memory and causes the nShield Connect to enter the self-test mode and perform their self test suites.

Logical Ports

Command Input

Configuration of the module is done from the front panel.

Configuration data is input using the control buttons and scroll wheel or using a keyboard attached to the USB port.

Authentication data is read from smart cards via the smart card interface.

Operators wanting to connect to the module send authentication commands via the Ethernet Port.

Data In

Data is input over the Ethernet Port, all traffic on this port is encrypted.

Data Out

Data is output over the Ethernet Port, all traffic on this port is encrypted.

Status Output

Status is output over

- the Ethernet Port
  status of returned jobs, all traffic on this port is encrypted.
- the front panel display
  the operator can select various status information using the front panel controls.
- the power switch
  the power switch is illuminated when the module is connected to mains power.
  Off, no mains power
  Flashing, standby on mains power
  On,
- the Warning LED
  Lit when the module needs attention after a tamper event or power supply failure.
- The Status LED
  Displays the current status of the nShield Connect.

Chapter 3: Excluded Components

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

The removable fan assembly

The fan assembly, including the backup battery is designed to be field replaceable if any of the fans fail or if the battery is discharged.

The module continuously monitor the status of all four fans and the backup battery.

The Power Supply Units

The module has two field replaceable power supply units that convert AC mains to 5V and 12V DC.

All voltages used internally are stepped down from this supply by separate power supplies which prevent fluctuation on the external power from affecting critical components.

Chapter 4: Roles

The module has the following roles:

Crypto-Officer

A user adopts the Crypto-Officer role by inserting a card into the card reader.

The nShield Connect verifies the card and reports the identity of the card to the module.

The module checks the identity of the card and if it belongs to a valid Crypto-Officer unlocks the front panel controls.

The Crypto-Officer can then select services from the menus displayed on the front panel of the nShield Connect.

User

An nCipher server running on a remote computer connects to the nShield Connect as a user, each server is identified by a DSA key pair - usually protected by an nToken.

The the Crypto-Officer must have configured the nShield Connect with the Ethernet address and identity of the operator.

The nCipher server sends a signed message to the nShield Connect to prove its identity. If the nShield Connect correctly verifies the message it uses Diffie-Hellman to establish a set of encryption and authentication keys to use on this channel.

Once this connection has been established, an application running on this computer can send commands to the nShield Connect.

Unauthenticated Role

A user who can access the front panel but who does not possess a valid smart card identifying themselves as a crypto-officer can see status information about the module, including which mode it is in, current status of temperature sensors and fans. However they cannot access any menus or perform any other services without authentication.

An nCipher server running on a remote server that has not been registered with the nShield Connect can open an unauthenticated connection and submit a public key and ethernet address. An authenticated crypto-officer.

Chapter 5: Services

Crypto-Officer Services

A Crypto-Officer at the front panel can use the menu system to access to the following services on the nShield Connect.

Service	Role	Description	Access to CSPs
Show Status	Any	Display module status	None
Network Configuration	Crypto-Officer	Configure the Ethernet settings for the module	None
Tamper Configuration	Crypto-Officer	Configure and reset the tamper circuit	None
Initialize Unit	Crypto-Officer	Initialize the module	**Generates** Module Signing key
Add Operator	Crypto-Officer	Add a new Operator ID (the operator's IP address and the hash of its public key) to the module configuration	**Imports** the Operator ID
Delete Operator	Crypto-Officer	Removes a Operator ID from the configuration	**Deletes** the Operator ID
Factory State (zeroize)	Crypto-Officer	Returns the module to the factory state, clearing all CSPs	**Zeroizes** all keys and CSPs
Shutdown	Crypto-Officer	Shuts down the module	**Deletes** session keys
Restart	Crypto-Officer	Restarts the module, causing it to rum all self tests	**Deletes** session keys
Firmware Upgrade	Crypto-Officer	Loads a new firmware image over the Ethernet interface After upgrading firmware the Crypto-Officer must re-initialize the nShield Connect.	**Uses** Firmware Integrity Key and Firmware Confidentiality key

User Services

An operator connecting over Ethernet interface has access to the following services:

Service	Role	Description	Access to CSPs
Authenticate	User	Verifies the operators identity and provides a signature with which the user can authenticate the identity of the module.	**Uses** Signing key, **Exports** signature and public key **Imports** the operator's public key and verifies key and signature.
Generate Keys		Establishes a set of encryption and authentication keys to use for this connection.	Generates ephemeral Key-exchange Key Establishes master secret by Diffie-Hellman key exchange with client **Establishes** Session keys from master secret.
Encrypt / Decrypt	User	Communicates with the operator over the secure channel	**Uses** Session keys
Show Status	Any	Display module status	None

Unauthenticated User

An unauthenticated user has access to the following services:

Service	Role	Description	Access to CSPs
Register	Any	Registers the ethernet address and hash of a public key for an new unauthenticated user - prior to a crypto officer using the Add User service to confirm them as valid users.	**Imports** hash of a public key
Show Status	Any	Display module status	None

Chapter 6: Keys

The following table summarizes the module's keys and CSP's:

Key	Type	Generation	Storage	Use	Zeroized	Role
Signing key	1024-bit DSA	Generated randomly according to FIPS 186-2.	Solid state hard drive	Identifies the nShield Connect to users	on tamper or when crypto officer selects factory state service	User
Key-exchange key	1024-bit Diffie Hellman	Generated randomly	DLG on Solid state hard drive Ephemeral keys in RAM	Key exchange in user authentication		
User's Public Keys	1024-bit DSA	Generated by User - generally using an nToken	Key hash stored on solid state hard drive Public key stored in RAM	Used to verify a signature to authenticate an individual user		
Session Keys	3 Key Triple DES	Established by Diffie Hellman Key exchange when a user authenticates	RAM	Encrypting and authenticating (Triple DES MAC) traffic from nShield Connect to user. Decrypting and verifying (Triple DES MAC) traffic from user to nShield Connect	when the connection closes, when new keys are established when the module is shutdown when crypto officer selects factory state service or on tamper.	
Firmware Integrity Key	ECDSA public key	Generated outside the module at Thales nCipher offices in Cambridge	Public Key: solid state hard drive Private Key: Stored securely at Thales nCipher offices	Identify valid firmware upgrade	No May be replaced during firmware upgrade	Crypto-Officer
Firmware Confidentiality Key	AES		Solid state hard drive	Encrypt firmware upgrade file		

Chapter 7: Setup and Initialization

In order to initialize the nShield Connect, the Crypto-Officer must take the following steps:

Setup Network Configuration

The Crypto-Officer must set the following values:

1. The IP Address for the nShield Connect.
2. The Net Mask
3. The Link Speed
4. The Default Gateway

The nShield Connect has two network connections which may be configured separately.

The Crypto-Officer may also configure specific routing information if this is required or their network.

The Crypto-Officer must restart the nShield Connect to incorporate any changes to network address or net mask.

Remote File System

The Crypto-Officer must specify the IP address of a server to use as a remote file system. This system stores a backup of the configuration data.

Before setting the RFS, the Crypto-Officer must set up the nCipher server on the remote operator to accept the connection from the nShield Connect.

Create a Operator

In order to comply with the requirements of FIPS 140-2 level 3. each operator must be fitted with a nToken, FIPS 140-2 certificate 967, 683 or 535, which will provide the cryptographic identity of the operator.

For each operator the Crypto-Officer must specify

5. the operator's IP address
6. the level of privileges (Unprivileged, Privileged on low ports, Privileged on any ports)

7. the hash of the hash of the operator's public key

Set up Front panel login control

To control access to front panel commands, the Crypto-Officer must enable front panel login control specifying the card set to use to identify the Crypto-Officer.

Once control has been enabled no front panel commands - except Show Status - can be access unless the Crypto-Officer logs in by inserting a card from the specified card set.

Configure nShield PCIe module

The crypto-officer must initialized nshield PCIe module in its FIPS 140-2 level 3 mode as described in the security policy for the nShield PCIe, FIPS certificate #1063

Determining the module is in FIPS mode

An user can determine whether the module is in FIPS mode by examining the menus displayed on the front panel display.

When the module is not configured in FIPS mode, the display shows the full set of menus whether or not a crypto officer is logged in - and there is no option to log out.

If the module is configured in FIPS mode and a Crypto-Officer has not logged in, the front panel display shows module status and a login prompt.

An unauthenticated user can scroll through the different status information (show status service) using the wheel but cannot access any other functions.

When a Crypto-Officer is logged in, the front panel displays the full menu structure which now includes a logout option. This option is not offered if the module is not in FIPS mode.

Chapter 8: Physical Security

The nShield Connect is fully encased by a two piece steel chassis consisting of a base and a lid. A steel wall separates the removable power supplies and fan assembly from the secure portion of the module.

All air vents are protected by baffles which ensure there is no direct access to the module.

There is no requirement to remove the lid. The replaceable parts can be removed with the lid in place.

The lid is held in place by four screws. There is a tamper evident seal, installed at the factory, on the top of the lid covering one of these screws. It is not possible to remove the lid without removing or damaging this label.

Figure 2 The Tamper Evident Label

Opening the lid is detected by tamper switches. The lid can only be removed by being slid backwards. There is sufficient overlap between the lid and base that the tamper switches will detect movement at a point where the lid still overlaps the base and before a gap opens that would allow access to circuitry.

The tamper circuitry monitors:

- lid switches
- backup battery voltages

If a tamper event is detected, the date and time of the event is recorded in the tamper log, and the module is reset to factory state.

A crypto-officer must reinitialized the module before it will return to the operational state.

The crypto-officer is instructed only to reinitialize the module if they are certain the tamper event is a false positive.

The crypto-officer must check the tamper seal at least once a month to ensure that it has not been removed or attacked.

Chapter 9: Strength of Functions

Operators are identified by their public key.

To authenticate a new operator, the crypto-officer compares the SHA-1 hash of the public key displayed on the front panel of the module with the value output by the nToken on the operator.

When a client initiates a connection, the module verifies a signature on a nonce using the public keys associated with the IP address. The signature is made with a 1024-bit DSA key using SHA-1. With is 1024-bit key there is one chance in 2^{80} or approximately one in 10^{24} of a false acceptance.

The module can process approximately one connection a second, or 60 a minute. Therefore the chance of a false acceptance in an minute is approximately one in 10^{22}.

Sessions are protected by a 168-bit Triple DES key - that is a Triple DES key with three independent keys, giving 112 bits of security.

In order to unlock the front panel, the Crypto-Officer must to insert a smart card from a specific Card Set.

The module verifies the SHA-1 hash of the logical token stored on the card. The chance of a false acceptance is therefore be one in 2^{80} or approximately one in 10^{24}.

It is impractical to make multiple attacks, as to do so the attacker would need to have control of another module in the same security world with which to make smart cards.

Chapter 10: 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 disables all input and output ports.

- An operational test on hardware components - including the full set of self tests on the nShield PCIe module.
- 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:
  - AES
  - Triple-DES
  - DSA
  - ECDSA
  - HMAC-SHA-1
  - HMAC-SHA-256
  - HMAC-SHA-512
  - Random Number Generator

If any of these tests fail the module enters the error state and I/O is disabled.

If all the tests pass the module starts the IP stacks allowing operators to make connections and enters the operational state.

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 is treated as a tamper event.

The module continuously monitors the state of the nShield module. If this module enters an error state so does the nShield Connect.

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

Firmware Load Test

When an Crypto-Officer 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.

In order to maintain FIPS 140-2 validation, only FIPS 140-2 validated firmware shall be loaded onto the module.

Chapter 11: FIPS approved and allowed algorithms:

The following table summarizes the algorithms used in the module:

Approved Security Function		**Certificate**
Symmetric		
AES	CBC	#1227
Triple DES	CBC	#883 (three key only)
SHA	SHA-1	#1127
	SHA-256	
	SHA-512	
HMAC	HMAC-SHA-1	#717
	HMAC-SHA256	
	HMAC-SHA512	
Asymmetric		
DSA		#407
ECDSA		#145
Random Number Generation		
RNG	FIPS 186-2 Change Note	#681
Allowed Security Function		
Diffie Hellman	Key agreement;	Key establishment methodology provide 80 bits of encryption strength.

The following table summarizes the algorithms provided by the nShield PCIe module within the nShield Connect module:

Approved Security Function		**Certificate**
Symmetric		
AES	ECB, CBC and CMAC	#754
	GCM Mode	AES Certificate #754 Vendor Affirmed
	CBC mode (Channel Open and Channel Update Services only)	#397
Triple DES	CBC	#666
	CBC mode (Channel Open and Channel Update Services only)	#435
SHA	SHA-1	#764
	SHA-224	
	SHA-256	
	SHA-384	
	SHA-512	
MAC	HMAC-SHA-1	#410
	HMAC-SHA256	
	HMAC-SHA512	
	AES GMAC	Vendor Affirmed
	Triple-DES MAC	Triple-DES Certificate #666 vendor affirmed
Asymmetric		
DSA		#280
RSA		#356
ECDSA		#81
Random Number Generation		
RNG		FIPS 186-2 Change Notice 1 SHA-1 and FIPS 186-2 RNG General Purpose RNG Certificate #436
Allowed Security Function		
Diffie Hellman	Key agreement	Key establishment methodology provides between 80 and 256 bits of encryption strength.
Elliptic Curve Diffie-Hellman	Key agreement	Key establishment methodology provides 192 bits of encryption strength.
Elliptic Curve MQV	Key agreement	Key establishment methodology provides between 80 and 256 bits of encryption strength.
SSL*/TLS master key derivation	Key establishment methodology	TLS key derivation is approved for use by FIPS 140-2 validated modules - though there is as yet no validation test.

Non-FIPS approved algorithms 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-Helman keys)
KCDSA	requires Feature Enable activation*
RSA*	encryption and decryption
Hashing and Message Authentication	
HAS-160*	requires Feature Enable activation
MD5*	MD5 may be used within TLS key derivation
RIPEMD 160*	
Tiger*	
HMAC*	MD5, RIPEMD160, Tiger
RNG	
Hardware RNG	used to provide entropy to seed approved pseudo-RNG

Addresses

Americas	Asia Pacific
2200 North Commerce Parkway Suite 200 Weston Florida 33326 USA Tel: +1 888 744 4976 or + 1 954 888 6200 sales@thalesesec.com	Units 2205-06 22/F Vicwood Plaza 199 Des Voeux Road Central Hong Kong PRC Tel: + 852 2815 8633 asia.sales@thales-esecurity.com
Australia	**Europe, Middle East, Africa**
103-105 Northbourne Avenue Turner ACT 2601 Australia Tel: +61 2 6120 5148 sales.australasia@thales-esecurity.com	Meadow View House Long Crendon Aylesbury Buckinghamshire HP18 9EQ UK Tel: + 44 (0)1844 201800 emea.sales@thales-esecurity.com

Internet addresses

Web site:	www.thalesgroup.com/iss
Support:	http://iss.thalesgroup.com/en/Support.aspx
Online documentation:	http://iss.thalesgroup.com/Resources.aspx
International sales offices:	http://iss.thalesgroup.com/en/Company/Contact%20Us.aspx