THALES

nToken Security Policy

www.thalesgroup.com/iss

Versions

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

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

Version	Date	Comments
2.4.2	10 June 2009	nShield PCI and nShield PCIe f/w 2.38.4
2.5.3	28 January 2010	nShield PCI and nShield PCIe f/w 2.33.82
2.5.4	17 February 2010	nShield PCI and nShield PCIe f/w 2.38.7
3.0	11 May 2012	nShield PCI and nShield PCIe f/w 2.50.17 - Thales branding

Contents

Chapter 1: Purpose

The nToken is a FIPS 140-2 level 2 module with level 3 physical security. It is designed to protect a single DSA key used to identify a host to a netHSM or nShield Connect.

The only purpose of the nToken is to sign a message containing a nonce to prove to the netHSM or nShield Connect that the session was instigated by a client running on the host.

nTokens are defined as multi-chip embedded cryptographic modules as defined by FIPS PUB 140-2.

Unit ID	Model Number	RTC NVRAM	SEE	Potting	EMC	Crypto Accelerator	Overall level
nToken	nC2023P-000	No	No	Yes	A	None	2

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

The module runs firmware provided by Thales. There is the facility for the administrator to upgrade this firmware. In order to determine that the module is running the correct version of firmware they should use the Show Status service which reports the version of firmware currently loaded. The validated firmware version is 2.50.16.

Provided that the nToken is only used with the FIPS approved firmware, it can only be operated in its FIPS approved mode of operation. It is possible to load new firmware. The administrator should ensure that any new firmware is FIPS validated before they load it into the module.

The nToken connects to the host computer via a PCI bus. The nToken must be accessed by a custom written application.

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

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

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

Initializing the nToken

When the module is initialized it generates a random AES key for use as a module key. This key is stored in the modules EEPROM and is never revealed. This step is usually performed in the Thales factory.

In order to enrol an nToken, the administrator runs the **nTokenEnrol** utility on a host computer, that is outside the security boundary.

The utility performs the following steps:

1. generates a DSA key pair (*Generate DSA key* service)
2. wraps the private half as a key blob protected by the module key (*Wrap key* service) and exports this blob to the host's hard disk.
3. exports a certificate containing the public key and the nToken's Electronic Serial number to the netHSM or nShield Connect. (*Export* service)
4. displays the SHA-1 hash of the DSA public key on the host computer's display, to enable the administrator to verify that they are enrolling the correct nToken. (*Hash* service)

The utility then sends this data to the netHSM or nShield Connect that will rely on the nToken. Once administrator confirms that the hash shown on the front panel display of the netHSM or nShield Connect is the same as that displayed at step 4, the netHSM or nShield Connect adds the nToken public key and serial number and the identity of the host in which it is installed to the it’s configuration file.

Using the nToken

Once the nToken is enrolled - whenever the Thales server is started it loads the key blob created when the module was initialized obtaining a key ID for the signing key.

The nToken is used when a operator wishes to open a connection from a host application to a netHSM or nShield Connect via the Thales server. When the operator attempts to open such a connection, the Thales server obtains a nonce from the netHSM or nShield Connect and has the nToken sign a message containing this nonce to confirm the identity of the computer the application is running on. The Thales server sends this message to the netHSM or nShield Connect. The netHSM or nShield Connect verifies the signature and can then determines whether the host is authorized.

Although the nToken uses the same firmware image as nShield modules, nToken modules are factory configured so that they can only perform a limited subset of operations. See Thales Master Feature Enable Key for more details.

The Thales server uses the Show Status service to determine which attached modules are nTokens and which are nShields. If the operator requests a service that the nToken cannot perform, the server ensures the command is routed to an nShield and not an nToken.

Upgrading Firmware

Although Thales do not expect that there will ever need to update the firmware in an nToken, Thales provide a utility to perform this.

Verifying firmware

The administrator or operator can use the **fwcheck** utility to check that the nToken has been programmed with valid firmware. This utility takes a copy of the signed and encrypted firmware file and performs a zero knowledge check to ensure the firmware loaded on the module is the same as the copy on disk.

Chapter 2: Excluded Components

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

- Standard 32-bit PCI interface
- mode links
- Reset switch
- Status LED

Chapter 3: Roles

The module has two roles which implicitly assumes all services:

Administrator

The Administrator Role is an implicitly assumed role that is procedurally assumed as part of the setup and initialization procedures of the nToken. The Administrator generates or replaces the secret AES Module Key. This step is performed by Thales before the module is shipped, but can be repeated by the customer as part of the setup and initialisation process.

Generates the signing key. To assume the administrator role, the administrator must run the nTokenEnrol utility. Running this utility implicitly selects the administrator role. This destroys all stored keys and creates a new key blob that is used to authenticate the user role and exports the public key that can be used to verify messages.

After the module has been configured, and is operating in its FIPS mode, there is no further requirement for the administrator role to interact with the module and all further services interaction is are performed in the implicitly assumed Administrator / User Role.

User

The user role uses the key to sign messages.

To assume the user role, the operator must present the key blob generated by the administrator. If this blob load correctly the module returns an **ObjectID** for the signing key. To sign a message the operator sends the **Sign** command with the **KeyID** and message. The module returns the signed message.

Chapter 4: Services

The following services are provided by the nToken.

Service	Key type	Role	Description
Check Firmware	DSA and AES	Admin / User	Performs a zero knowledge check of the firmware image.
Generate Key	AES	Admin	The module automatically generates a new AES key used as the module key. This key is never exported. This is performed as part of the setup and initialisation procedure.
Generate Key	DSA	Admin	The module generates a DSA key pair, used to sign messages. This is performed as part of the setup and initialisation procedure.
Wrap Key	AES + HMAC	Admin	The private DSA key is wrapped as an Thales key blob. Wrapping uses AES CBC mode for encryption and SHA-1 HMAC for integrity. This is performed as part of the setup and initialisation procedure.
Export	DSA public	Admin	The public half of the DSA key pair is exported in plain text. This is performed as part of the setup and initialisation procedure.
Hash	SHA-1	Admin	The module exports the SHA-1 hash of the DSA key to enable the key to be identified in other services. The hash can be calculated from either the private or public half of the key. This feature can be used to ensure the correct parts of a key pair are being used. This is performed as part of the setup and initialisation procedure.
Unwrap Key	AES + HMAC	User	The operator presents the wrapped private key at the start of a session. If the key unwraps and the MAC verifies, the operator is authorized.
Sign	DSA private	User	Once the operator has loaded the private key they can use it to sign messages.
Zero	DSA private	Admin / User	Clears all unwrapped keys. The Module key can be zeroed by repeating the Key Generation Service.

Service	Key type	Role	Description
Show Status		Admin / User	Displays status information.
Loads Firmware	DSA and AES	Admin	Replaces a firmware image with new firmware. The firmware is signed and encrypted with keys held at Thales. The nToken must be re-initialized after loading firmware.

Chapter 5: Keys

For each type of key used by the nToken, the following section describes the access that a operator has to the keys. The nToken refers to keys by their handle, an arbitrary number, or by its SHA-1 hash.

Module keys

The Module key is an AES key used to protect other keys. This key is generated by the module key when it is initialized. If the module is re-initialized, the AES key is cleared and a new key must be generated before the module can be started in operational mode. nTokens are initialized by Thales before they are supplied to the customer and do not normally need re-initializing. The module key is guaranteed never to have been known outside this module.

Authentication Key

When the nToken is enrolled it generates a DSA key pair used for signature generation. The public half of this key is exported in plain text and has to be transferred to the netHSM or nShield Connect.

The private half is encrypted under the module key and exported as an Thales format key blob which is stored on the host computer's hard disk.

In order to use the signature key, the operator loads the key blob. When the key is loaded in the module it is stored in RAM and identified by a random identifier that is specific to the operator and session. The operator can then have the module sign messages by providing this identifier.

Firmware Integrity Key

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

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

The private half of this key is stored at Thales.

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

Firmware Confidentiality Key

All firmware is encrypted using AES to prevent casual decompilation.

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

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

Master Feature Enable Key

The nToken uses the same firmware and basically the same hardware as the Thales nForce and nShield modules. However most functionality is disabled using Thales's Feature Enable Mechanism. This controls features using certificates signed by the Thales Master Feature Enable Key. Presenting such a certificate causes the module to set the appropriate bit in the FRAM.

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

DRBG Key

The module uses the CTR_DRBG from SP800-90 with a 256-bit AES key. This key is seeded from the on board entropy source whenever the module is initialised and is reseeded according to SP800-90 with a further 512-bits of entropy after every 2048-bytes of output.

This key is only ever used by the DRBG. It never exposed outside the module.

Chapter 6: Rules

Object re-use

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

Error conditions

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

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

Security Boundary

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

All cryptographic components are covered by potting.

Some items are excluded from FIPS 140-2 validation as they are not security relevant see Excluded Components on page 9.

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.

Chapter 7: Physical security

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

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

Checking the module

To ensure physical security, make the following checks regularly:

Examine the epoxy resin security coating for obvious signs of damage.

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

Chapter 8: Strength of functions

Attacking Object IDs

A operator is authenticated by a key blob, which is encrypted by a 256-bit AES key with integrity provided by a 160-bit HMAC key. It is therefore almost impossible to spoof this authentication.

An attacker may however get the module to sign a message with the stored key by guessing the client and key identifiers.

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 that the required chance of 1 in 10^{5} ($\sim 2^{-17}$)

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.

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

An operational test on hardware components

An integrity check on the firmware, verification of a SHA-1 hash.

A statistical check on the random number generator

Known answer and pair-wise consistency checks on all approved and allowed algorithms in all approved modes and of the DRBG

Verification of a MAC on FRAM contents to ensure it is correctly initialized.

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

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

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

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

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

Chapter 10: Supported Algorithms

Algorithms marked with an asterisk (*) are not enabled when the module is configured as a nToken.

FIPS approved and allowed algorithms:

Symmetric Encryption

- AES
  Certificate #1579
  ECB, CBC GCM* and CMAC* modes

- Triple-DES*
  Certificate #1035
  ECB and CBC mode

Hashing and Message Authentication

- AES CMAC*
  AES Certificate #1579

- AES GMAC*
  AES Certificate #1579

- HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384 and HMAC SHA-512
  Certificate #925

- SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512
  Certificate #1398

- Triple-DES MAC*
  Triple-DES Certificate #1035 vendor affirmed

Signature

- DSA
  Certificate #487
  FIPS 186-2 and FIPS 186-3 signature generation and verification
  Modulus 1024-bits Sub-group 160-bits SHA-1
  Modulus 2048-bits Sub-group 224-bits SHA-224
  Modulus 2048-bits Sub-group 256-bits SHA-256
  Modulus 3072-bits Sub-group 256-bits SHA-256

- ECDSA*
  Certificate #192
  FIPS186-2: Signature Generation and Verification
  P-192 P-224 P-256 P-384 P-521 K-163 K-233 K-283 K-409 K-571 B-163 B-233 B-283 B-409 and B-571 Curves

- RSA*
  Certificate #770
  RSASSA-PKCS1_V1_5 signature generation and verification
  Modulus 1024 - 4096 bits with SHA-1, SHA-224, SHA-256,SHA-384 and SHA-512

Key Establishment

- Diffie-Hellman *
  (CVL Cert. #1, key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength)

- Elliptic Curve Diffie-Hellman *
  (CVL Cert #1, key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength)

- EC-MQV *
  (key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength)

- RSA *
  (key wrapping, key establishment methodology provides between 80 and 256 bits of encryption strength)

- AES *
  (AES Certificate #1579, key wrapping; key establishment methodology provides between

128 and 256 bits of encryption strength)
AES Key Wrap, AES CMAC Counter mode according to SP800-108, AES CBC mode

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

Other

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

Non-FIPS approved algorithms

Symmetric

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

Asymmetric

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

Hashing and Message Authentication

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

Non-deterministic entropy source

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

Other

SSL*/TLS master key derivation

PKCS #8 padding*.

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

Thales addresses

Americas

2200 North Commerce Parkway
Suite 200
Weston
Florida 33326
USA

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

sales@thalesesec.com

Asia Pacific

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

103-105 Northbourne Avenue
Turner
ACT 2601
Australia

Tel: +61 2 6120 5148

sales.australasia@thales-esecurity.com

Europe, Middle East, Africa

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