FIPS 140-2 Level 3 Security Policy

NITROX XL 1600-NFBE Family

Document number: CN16xx-NFBE-SPD-L3
Version: Version 1.1
Revision Date: 6/7/2010

Revision History

Revision	Date	Author	Description of Change
0.001	08/12/2009	Prasad Vellanki	Initial Draft
0.002	10/16/2009	Prasad Vellanki	Changes to the cloning procedure to include ECC
0.003	10/30/2009	Prasad Vellanki	Incorporated review comments
0.004	11/5/2009	Prasad Vellanki	Incorporated workshop comments
0.4.4	12/13/2009	Prasad Vellanki	Incorporated comments from Andrei
1.0	1/14/2010	Prasad Vellanki	Final Changes
1.1	6/11/2010	Prasad Vellanki	Incorporated comments from Andrei

Table of Contents

1. Module Overview 5
2. Security Level 7
3. Modes of Operation 8
3.1. FIPS Approved Mode of Operation 8
3.2. Non-FIPS Mode of Operation 8
3.3. Approved and Allowed Algorithms 8
3.4. Non-Approved, Non-Allowed Algorithms 9
3.5. LED Error Pattern for FIPS failure 9
4. Ports and Interfaces 11
5. Identification and Authentication Policy 12
5.1. Assumption of Roles 12
6. Access Control Policy 14
6.1. Roles and Services 14
6.1.1. Cryptographic Officer (CO) Services 14
6.1.2. CU services 14
6.1.3. Unauthenticated Services 15
6.2. Definition of Critical Security Parameters (CSPs) 17
6.3. Definition of Public Keys 18
6.4. Definition of CSPs Modes of Access 19
7. Operational Environment 20
8. Security Rules 21
9. Physical Security Policy 22
9.1. Physical Security Mechanisms 22
10. Mitigation of Other Attacks Policy 22
11. References 23
12. Definitions and Acronyms 23

List of Tables

Table 1 – Module Security Level Specification ... 7
Table 2 – FIPS Approved Algorithms Used in the Module ... 8
Table 3 – FIPS Allowed Algorithms Used in the Module ... 9
Table 4 – Non-Approved, Non-Allowed Algorithms Used in the Module ... 9
Table 5 – Cavium HSM Ports and Interfaces ... 11
Table 6 – Roles and Required Identification and Authentication ... 12
Table 7 – Strengths of Authentication Mechanisms ... 13
Table 8 – Authenticated Services (CO only) ... 14
Table 9 – Authenticated Services (CU only) ... 14
Table 10 – Unauthenticated Services ... 15
Table 11 – Specification of Service Inputs & Outputs ... 15
Table 12 – Private Keys and CSPs ... 17
Table 13 – Public Keys ... 18
Table 14 – CSP Access Rights within Roles & Services ... 20

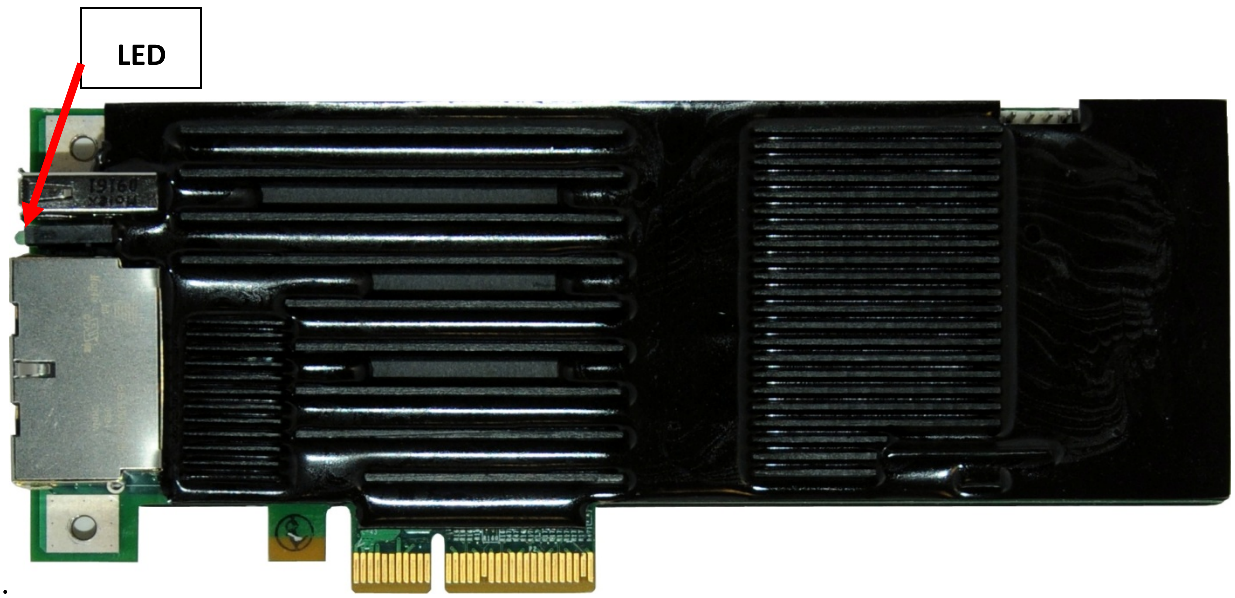
List of Figures

Figure 1 – Top View of Cryptographic Module ... 5
Figure 2 – Bottom view of Cryptographic Module ... 6

1. Module Overview

The Cavium Networks NITROX XL 1600-NFBE HSM Family (hereafter referred to as *the module or HSM*) is a high performance purpose built security solution for crypto acceleration. The module provides a FIPS 140-2 overall Level 3 security solution. The module is deployed in a PCIe slot to provide crypto and TLS 1.0 acceleration in a secure manner to the system host. It is typically deployed in a server or an appliance to provide crypto offload. The module's functions are accessed over the PCIe or Ethernet interface via an API defined by the module.

The module is a hardware multi-chip embedded cryptographic module. The module provides cryptographic primitives to accelerate approved and allowed algorithms for TLS 1.0 and SSH. The cryptographic functionality includes modular exponentiation, random number generation, and hash processing, along with protocol specific complex instructions to support TLS 1.0 security protocols using the embedded NITROX chips. The module implements single and two factor authentication at FIPS 140-2 Level 3 security. The physical boundary of the module is implemented by an epoxy enclosure.



.

Figure 1 – Top View of Cryptographic Module

Figure 2 – Bottom view of Cryptographic Module

The configuration of hardware and firmware for this validation is:

Hardware Version: 2.0

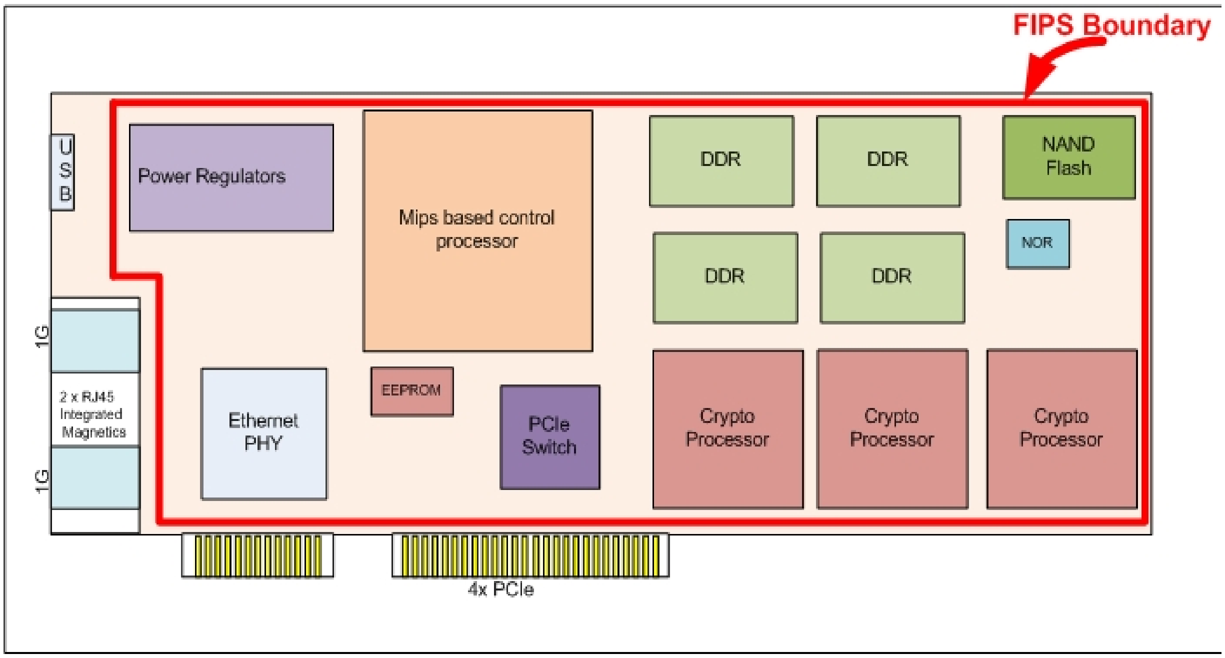
Hardware Part Numbers:

- NIC version
  - CN1620-NFBE1NIC-2.0-G
  - CN1620-NFBE2NIC-2.0-G
  - CN1620-NFBE3NIC-2.0-G
  - CN1610-NFBE1NIC-2.0-G
- Non-NIC version
  - CN1620-NFBE1-2.0-G
  - CN1620-NFBE2-2.0-G
  - CN1620-NFBE3-2.0-G
  - CN1610-NFBE1-2.0-G

Firmware: Version 1.1

The module supports the performance options listed above in the hardware identifier. The physical hardware and firmware are identical across all options. The underlying hardware has multiple identical cryptographic engines which are enabled or disabled using an option parameter set at manufacturing time.

The major blocks of the module are: General purpose MIPS based control processor, Crypto processors, RAM memory, NOR and NAND for persistent storage, Ethernet and USB interfaces, and PCIe x4 interfaces.



2. Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

Table 1 – Module Security Level Specification

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

3. Modes of Operation

The module supports the following modes of operation –

1) Non-FIPS mode of operation
2) FIPS Approved Level 3 mode of operation

The module is initialized into one of the modes specified above during the module initialization period. The value of the parameter fipsState passed into the call specifies the mode. Following are the allowed values for fipsState parameters:

0 - Non-FIPS mode

1 - FIPS Approved mode single factor authentication mechanism

2 - FIPS Approved mode two factor authentication mechanism

The indicator of Approved mode is obtained by using the Get Status service. The fipstate field of Get Status service indicates the mode. The module is required to be zeroized before reconfiguration to a different mode of operation.

3.1. FIPS Approved Mode of Operation

The module provides a FIPS Approved mode of operation, comprising all services described in Sections 6.4 and 6.4 below. In this mode, the module allows only FIPS Approved or allowed algorithms. Request for any non Approved/allowed algorithm is rejected.

3.2. Non-FIPS Mode of Operation

The Module supports a Non-FIPS mode implementing the non-FIPS Approved algorithms listed in Table 4.

3.3. Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithms.

Table 2 – FIPS Approved Algorithms Used in the Module

FIPS Approved Algorithm	Usage	Certificate
AES: CBC; 128, 192, 256 bits	Data encryption and decryption, key wrap	1265
AES: ECB CTR 256 bits	DRBG	1266
Triple-DES: CBC; 168 bits	Data encryption and decryption	898
RSA 1024, 2048, 4096	Authentication, Key Transport, Signature Verification, Key generation	607
ECDSA PKG	Key Generation, public key validation	150
SHA1:160; SHA2: 256, 384, 512	Secure hashing	1165
SHA1:160; SHA2:512	Signature verification	1166
HMAC: SHA2: 512	Message integrity	736
KAS – SP800-56A (ECC)	Key agreement	5
RNG – ANSI X9.31	Deterministic random number generation	707

SP800-90 CTR DRBG	Deterministic random number generation	32

The cryptographic module supports the following non-FIPS Approved algorithms which are allowed for use in FIPS mode. ECC key pair generation is done as per Appendix B.4.1 key pair generation.

Table 3 – FIPS Allowed Algorithms Used in the Module

Algorithm	Usage
Hardware RNG (NDRNG)	Seed, seed key generation
RSA PKCS#1 2048 (key wrapping; key establishment methodology provides 128 bits of encryption strength)	CSP Encrypt/Decrypt
AES Key Wrap per NIST Specification (key wrapping; key establishment methodology provides 256 bits of encryption strength)	Key Transport

The support of TLS 1.0 protocol by the module is restricted to the TLS Key Derivation Function and the crypto operation. This functionality of the module is used by the user of the module as part of TLS protocol negotiation.

3.4. Non-Approved, Non-Allowed Algorithms

The cryptographic module supports the following non-Approved algorithms available only in non-FIPS mode.

Table 4 – Non-Approved, Non-Allowed Algorithms Used in the Module

Algorithm	Usage	Keys/CSPs
RC4	Encryption/Decryption	RC4 key of 128 bits
MD5	Hashing	N/A
PBE	Key generation	Password

3.5. LED Error Pattern for FIPS failure

The blink pattern (ON then OFF, X times) followed by a blink gap delay of 200 ms are kept for easy identification of the error on the HSM.

All blinks are 50msec ON and 50 msec OFF.

	Cycles (X)
AES (Encrypt, Decrypt)	1
Triple-DES (Encrypt, Decrypt)	2
SHA 160, 256, 512 (Hardware)	3
RSA Sig Ver	4
RSA Key Gen	5

RSA Enc/Dec	6
RNG (ANSI 9.31 KAT)	7
SHA 512 (Firmware)	8
HMAC SHA512 (Firmware)	9
DRBG (SP-800-90 KAT)	10
ECDSA Key Gen	11
ECDSA PKV	12
KAS (IG9.6) KAT	13
AES ECB (Encrypt, Decrypt Hardware)	14
HMAC (SHA169, SHA256, SHA384, SHA512)	15
DRBG continuous number test	10
ECDSA PKV Conditional Test	12
Hardware RNG continuous number test	24
ECDSA Pairwise Consistency Conditional Test	25
Conditional Load Test (RSA Sig Ver)	4

On successful completion of the FIPS tests, the LED remains in the “ON” state. Blinking indicates failures on the HSM. If the LED remains in the permanent glow, the card’s state is fine.

4. Ports and Interfaces

The module ports and interfaces are:

Table 5 – Cavium HSM Ports and Interfaces

Physical Ports/Interface	Pins Used	FIPS 140-2 Designation	Name and Description
Gigabit Ethernet (2)	Ethernet Transmit/Receive standard interface (bidirectional pairs) leading to a standard RJ-45 pinout Pins (1,2), (3,6), (4,5), (7,8)	Data Input Data Output	Ethernet Interface - Used for Level 3 authentication - Used as NIC interface for the host the module is plugged into (passthrough)
USB Interface	USB Interface USB0_DP, USB0_DM	Power No functionality in FIPS mode	USB Interface Used for public key loading during initialization period only; not used in FIPS mode
Serial Interface	4 Pin serial interface - GND, 3.3V, Tx, Rx	N/A No functionality in FIPS mode	Disabled at the hardware level once the module has completed the initialization period.
PCIe Interface	PCIE x4 Interface Lane 0 Transmit Side B (14, 15) Receive Side A (16, 17) Lane 1 Transmit Side B (19, 20) Receive Side A (21, 22) Lane 2 Transmit Side B (23, 24) Receive Side A (25, 26) Lane 3 Transmit Side B (27, 28) Receive Side A (29, 30)	Data Input Control Input Data Output Status Output Power	PCIe Interface - Primary interface to communicate with the module - Provides APIs for the software on the host to communicate with the module
LED	LED interface (2 pins)	Status output	Visual status indicator

5. Identification and Authentication Policy

5.1. Assumption of Roles

The module supports two distinct operator roles, Cryptographic User (CU) and Cryptographic Officer (CO). The module enforces the separation of roles using identity-based authentication. Re-authentication is required to change roles. Concurrent operators are allowed; however, only one operator is allowed per login session.

The User Id is used as the identification for identity-based authentication. The module supports two different authentication schemes based on the initial module configuration:

- Single factor password based authentication: Username and the password encrypted with 2048 bit RSA public key is passed during the Login service.
- Two factor password and challenge/response authentication: Username and encrypted password are supplied during the Login service, followed by a cryptographic challenge response mechanism.

Table 6 – Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
CO	This role has access to administrative services offered by the module.	Identity-based operator authentication	Single factor: 7 to14 character encrypted password. Two factor: 1) 7 to14 character encrypted password 2) An RSA 1024 signed challenge.
CU	This role has access to all crypto services offered by the module. These services include login, create, delete, import, and export CSPs on the module.	Identity-based operator authentication	Single factor: 7 to14 character encrypted password. Two factor: 1) 7 to14 character encrypted password 2) An RSA 1024 signed challenge.

Table 7 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Single Factor Authentication using password based scheme	Single factor authentication provides a false acceptance rate of 1/78,364,164,096 less than 1/1,000,000), determined by the password. Password is minimum 7 characters, alpha-numeric so it is (26+10)^7 To exceed 1 in 100,000 probability of a successful random attempt during a 1-minute period, 7350919 (122515 per second) attempts would have to be executed. The module limits the number of Login tries to a user configured value "login_fail_count" during module initialization. This configuration value cannot exceed 20. If the user exceeds the configured value for maximum consecutive failed login attempts then the module is zeroized.
Two-factor authentication using password scheme and RSA public key cryptography	Two factor authentication is in excess of the false acceptance rate requirement. The analysis for single factor authentication above holds, with the addition of a cryptographic challenge response. The module limits the number of Login tries to a user configured value "login_fail_count" during module initialization. This configuration value cannot exceed 20. If the user exceeds the configured value for maximum consecutive failed login attempts then the module is zeroized.

6. Access Control Policy

The Cryptographic Hardware Security Module enforces identity-based authentication. A role is explicitly selected at authentication; either Crypto Officer (CO) or Crypto User (CU) is valid. The module allows one identity per role.

6.1. Roles and Services

6.1.1. Cryptographic Officer (CO) Services

The following table lists the services. Each service is implemented using one or more of the API functions.

Table 8 – Authenticated Services (CO only)

Service	Description
Firmware Upgrade	Allows the CO to upgrade the firmware after the firmware integrity check. New firmware is out of scope of this validation; as the module's validation to FIPS 104-2 is no longer valid once any non-validated firmware is installed
Clone Masking Key	Securely clones the Masking key between the modules which is used to encrypt backup CSPs from the module
Performance Configuration	Allows the CO to set the performance configuration
Generate KLK	Generate KLK
Generate MAC	Generate a message authentication code using HMAC
Change CO Password	Changes CO password
Logout	Logs out the operator (returns the module to the unauthenticated state) and closes the session
Encrypt/Decrypt Data	Encrypt and Decrypt data using keys in the module
Show Status	Display the status of the module like configuration, FIPS Approved mode, free memory, used sessions. Fipsstate field indicates the mode of operation for the HSM.
Session Status	Show the login status of the session
Zeroize Module	Zeroizes all plaintext CSPs in the module by overwriting memory in all locations
Power Cycle	Power Cycle the module

6.1.2. CU services

Table 9 – Authenticated Services (CU only)

Service	Description
Key and Key Pair Management	Generate, Import, delete and change label of symmetric and asymmetric keys. Outputs plaintext public key.
Secure Backup / Restore	Mask and unmask symmetric and asymmetric keys using masking key in the module
Encrypt/Decrypt Data	Encrypt and Decrypt data using keys in the module
Secure Key Load	Enter CSPs into the module in encrypted form

Generate MAC	Generate a message authentication code using HMAC
Change CU Password	Changes CU password
Logout	Logs out the operator (returns the module to the unauthenticated state) and closes the session
Show Status	Display the status of the module like configuration, FIPS Approved mode, free memory, used sessions. Fipsstate field indicates the mode of operation for the HSM.
Session Status	Show the login status of the session
Zeroize Module	Zeroizes all plaintext CSPs in the module by overwriting memory in all locations
Power Cycle	Power Cycle the module

6.1.3. Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 10 – Unauthenticated Services

Service	Description
Login	Allows the operator to authenticate to the module
Show Status	Display the status of the module like configuration, FIPS Approved mode, free memory, used sessions. Fipsstate field indicates the mode of operation for the HSM.
Session Status	Show the login status of the session
Session Close	Closes the session
Zeroize Module	Zeroizes all plaintext CSPs in the module by overwriting memory in all locations
Power Cycle	Power Cycle the module

The following table describes the input/output arguments and the return values from all the services. All the inputs and outputs - Data and Control, are exchanged over PCIe interface.

Table 11 – Specification of Service Inputs & Outputs

Service	Control Input	Data Input	Data Output	Status Output
Login	Session Handle	User Name, Encrypted Password, Nonce	N/A	SUCCESS/FAILURE
Show Status	Session Handle	Flags	Session Status	SUCCESS/FAILURE
Session Status	Session Handle	N/A	Login Status	SUCCESS/FAILURE
Session Close	Session Handle	N/A	N/A	SUCCESS/FAILURE
Zeroize Module	Session handle	NA	N/A	SUCCESS/FAILURE
Power Cycle	N/A	N/A	N/A	SUCCESS
Key and Key pair management	Session handle	Key handle	Encrypted key Plain Public key	SUCCESS/FAILURE
Secure Backup/Restore	Session Handle	Key Handle	Wrapped Key	SUCCESS/FAILURE

Encrypt/Decrypt Data	Session handle	Plain Data, Key handle	Encrypted Data	SUCCESS/FAILURE
Secure Key Load	Session Handle	Encrypted CSP	Key Handle	SUCCESS/FAILURE
Generate MAC	Session handle	Data, Key Handle	MAC on Data	SUCCESS/FAILURE
Change CU Password	Session Handle	Encrypted old and new passwords	N/A	SUCCESS/FAILURE
Logout	Session Handle	N/A	N/A	SUCCESS/FAILURE
Generate KLK	Session Handle	Source HSM Public Key, Target HSM Public Key, Nonce	Encrypted Masking Key	SUCCESS/FAILURE
Performance Configuration	Session Handle	Performance Level, Signature	N/A	SUCCESS/FAILURE
Change CO Password	Session Handle	Encrypted old and new passwords	N/A	SUCCESS/FAILURE
Clone Masking Key	Session Handle	Source HSM Public Key, Target HSM Public Key, Nonce	Encrypted Masking Key	SUCCESS/FAILURE
Firmware Upgrade	Session Handle	Firmware file, Signature file	N/A	SUCCESS/FAILURE

6.2. *Definition of Critical Security Parameters (CSPs)*

Master Key is stored in the EEPROM while all other CSPs are encrypted using Master Key and stored in the persistent memory. The User Login Public Keys for Crypto User (CU) and Crypto-Officer (CO) are generated on smart card and imported to store in modules persistent memory. The following table lists the CSPs contained in the module.

Table 12 – Private Keys and CSPs

Key Name	Type	Description
RNG Internal State (XKEY, XSEED)	Input to AES256 whitening function	XKEY and XSEED.
DRBG Internal State	Input to AES256 CTR mode whitening function	Counter, entropy input, nonce, and personalization input.
Master Key	AES-256 key	Used to encrypt and decrypt a subset of CSPs stored in the module.
KBK	AES-256 key	Used to encrypt the CSPs to extract the keys out of the module.
KLK (Key Loading Key)	AES-256 key	Used to decrypt the imported CSPs.
Cloning Private Key	512 bit ECDSA Private key	Used for key agreement of clone module service
Cloning Shared Secret (Z)	Random number	Output from the Approved KDF.
Clone Session Encryption Key	AES-256 key	Generated as part of key agreement scheme and used for wrapping masking key during clone module service.
Key Loading Private Key	512 bit ECDSA Private key	Used for key agreement of key import service to derive KLK.
Key Loading Shared Secret (Z)	Random number	Output from the Approved KDF.
Crypto User Password	7 to 14 Characters	Entered into the module during the user creation. The password is compared during the Login service to authenticate the CU.
Crypto-Officer Password	7 to 14 Characters	Entered into the module during the user creation. The password is compared during the Login service to authenticate the CO.
PSWD_DEC Private Key	2048-bits RSA private key	Used to decrypt the user supplied encrypted password during user creation and login.
RSA Private Key	RSA key of 1024, 2048, 4096 bits	Generated, imported or inserted into the module using the module services.
Triple-DES Symmetric Keys	Set of Triple-DES-168 keys	Generate, transported or entered into the module using the module services under the control of authenticated (CO or CU) operators. If generated on the module, generated with an Approved RNG. If transported or entered, the module uses key transport of 256 bits of strength.
AES Symmetric Keys	Set of AES-128, 192, 256 keys	Generate, transported or entered into the module using the module services under the control of authenticated (CO or CU) operators. If generated on the module, generated with an Approved RNG. If transported or entered, the module uses key transport of 256 bits of strength.

Key Name	Type	Description
HMAC-SHA Key	Random number	Secret key used to generate HMAC-SHA MAC data.
TLS 1.0 Session AES Symmetric Key	AES 128, 192, 256	Generated as part of the TLS 1.0 protocol negotiation.
TLS 1.0 Session Triple-DES Symmetric Key	3_DES 192	Generated as part of the TLS 1.0 protocol negotiation.
TLS 1.0 Session MAC Key	SHA-1 key	Generated as part of the TLS 1.0 protocol negotiation.
Clone Session MAC Key	SHA-256 MAC key	Generated as part of key agreement scheme and used as key confirmation during clone module service.

6.3. Definition of Public Keys

The module contains the following public keys:

Table 13 – Public Keys

Key Name	Type	Description
SW/FW Validation Key	1024 bits RSA public key	Used to validate the firmware upgrade and Manufacturer provided static configuration.
License Key	1024 bits RSA public key	used to validate the license service for module configuration (1, 2, 3, 4 module configurations).
Password Encryption Public Key	2048 bits RSA public key	Used encrypt the user passwords during user creation and login.
Cloning Initiator Public Key	ECC 512 bit Static public key	Used in SP 800-56A C(0,2,ECC DH) key agreement to generate shared secret Z. At HSM level, used to establish secure channel for cloning process (to export Masking Key).
Cloning Responder Public Key	ECC 512 bit Static public key	Used in SP 800-56A C(0,2,ECC DH) key agreement to generate shared secret Z. At HSM level, used to establish secure channel for cloning process (to export Masking Key).
Key Load Initiator Public Key	ECC 512 bit Static public key	Used in SP 800-56A C(0,2,ECC DH) key agreement to generate shared secret Z. At HSM level, used to establish secure channel for importing encrypted CSPs (Secure Key Loading).
Key Load Responder Public Key	ECC 512 bit Static public key	Used in SP 800-56A C(0,2,ECC DH) key agreement to generate shared secret Z. At HSM level, used to establish secure channel for importing encrypted CSPs(Secure Key Loading).
CO Login Public Key	1024 bits RSA public key	Used for signature verification in a challenge / response protocol during Login process as an optional second authentication factor.
CU Login Public Key	1024 bits RSA public key	Used for signature verification in a challenge /

Key Name	Type	Description
		response protocol during Login process as an optional second authentication factor.
Cloning Domain Parameter Set	ECC P-512 curve domain parameters	Domain parameter set D (Set EE) ECC P-512 curve domain parameters used in SP 800-56A C(0,2,ECC DH) key agreement to derive shared secret Z.

6.4. Definition of CSPs Modes of Access

Table 13 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

G = Generate: The module generates the CSP.

R = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.

W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, or the module generates a CSP, or the module overwrites an existing CSP.

Z = Zeroize: The module zeroizes the CSP.

Table 14 – CSP Access Rights within Roles & Services

Role	Service	Mode	Cryptographic Key or CSP
Unauthenticated	Login	R	Password Encryption public Key, Crypto User Password, Crypto-Officer Password
Unauthenticated	Show Status	None	None
Unauthenticated	Session Status	None	None
Unauthenticated	Session Close	None	None
Unauthenticated	Zeroize Module	Z	All CSPs
CO	Firmware Upgrade	R	SW/Firmware Validation Key
CO	Performance Configuration	R	License Key
CO	Generate KLK	G, R	Key Load Initiator Public Key, Key Load Responder Public Key, Key Loading Private Key, KLK
CO	Change CO Password	R	Password Encryption public Key, Crypto User Password, Crypto Officer Password
CO	Clone Masking Key	G, R	Cloning Initiator Public Key, Cloning Responder Public Key, Cloning Private Key, KBK
CO	Generate MAC	R	MAC Key
CO	Logout	None	None
CO	Encrypt/Decrypt Data	R	Symmetric Key: TDES, AES Asymmetric Key RSA
CU	Key and Key Pair Management	G, R, Z	Symmetric Key: AES, TDES Asymmetric Key: RSA Password Encryption public key
CU	Secure Backup/Restore	R, RZ, W	KBK, Symmetric Key/Asymmetric Key
CU	Secure Key Load	R, W	Key Load Initiator Public Key, Key Load Responder Public Key, Key Load private key, KLK , Key Object
CU	Generate MAC	R	MAC Key
CU	Change CU Password	R	Password Encryption public Key, Crypto User Password, Crypto Officer Password
CU	Logout	None	None
CU	Encrypt/Decrypt Data	R	Symmetric Key: TDES, AES Asymmetric Key: RSA

7. Operational Environment

The module implements a limited operational environment. FIPS 140-2 Area 6 Operational Environment requirements do not apply to the module in this validation.

8. Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level-3 module.

1. The cryptographic module clears previous authentications on power cycle
2. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
3. The cryptographic module shall perform the following power up, continuous and conditional self-tests

   A. <u>Power-Up Tests</u>
   - AES Encrypt & Decrypt KATs
   - Triple-DES Encrypt & Decrypt KAT
   - SHS KAT 160 bit (hardware implementation)
   - RSA SigVer and KeyGen KAT
   - HMAC-SHA-512 KAT (firmware implementation)
   - RNG ANSI X9.31 KAT
   - SHS KAT 160, 256, 512 (firmware implementation)
   - SP800-90 CTR_DRBG KAT
   - ECDSA KeyGen and PKV KAT
   - RSA Encrypt & Decrypt KAT
   - KAS KAT per IG 9.6 (Q=dG and KDF)
   - Firmware integrity test (CRC16)

   B. Conditional Self-Tests
   - ECDSA Pairwise Consistency Test
   - RSA Pairwise Consistency Test
   - ANSI X9.31 Continuous number test
   - SP800-90 CTR_DRBG Continuous number test
   - KAS conditional test
   - Firmware load test (RSA SigVer KAT)
   - HW RNG Continuous Number Test
4. Critical Functions Tests: The module runs following Critical Functions Tests which are required to ensure the correct functioning of the device.
   a. Power On Memory Test
   b. Power On Phy Test
   c. EEPROM Test
   d. NOR Flash Test
   e. Nitrox Chips Tests
5. The operator shall be capable of commanding the module to perform the power up self-test by cycling power or resetting the module.
6. Power up self-tests do not require any operator action.
7. Data output shall be inhibited during self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

9. The module ensures that the seed and seed key inputs to the Approved RNG are not equal.
10. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
11. The module does not support a maintenance interface or role.
12. The module does not support bypass capabilities.
13. The module does not support manual key entry.
14. The module has no CSP feedback to operators.
15. The module does not enter or output plaintext CSPs
16. The module does not output intermediate key values.
17. The module shall be configured for FIPS operation by following the first-time initialization procedure described in User Manual and C-API Specification (CN16xx-NFBE-API-0.9)

9. Physical Security Policy

9.1. Physical Security Mechanisms

The module’s cryptographic boundary is defined to be the outer perimeter of the epoxy enclosure containing the hardware and software components. The module is opaque and completely conceals the internal components of the cryptographic module. The epoxy enclosure of the module prevents physical access to any of the internal components without having to destroy the module. There are no operator required actions.

10. Mitigation of Other Attacks Policy

No mitigation of other attacks are implemented by the module.

11. References

1. NIST AES Key Wrap Specification, 16th Nov, 2001.
2. NIST Special Publication 800-56A, March, 2007.
3. NIST Special Publication 800-57 Part-1, May 2006.
4. FIPS PUB 140-2, FIPS Publication 140-2 *Security Requirements for Cryptographic Modules*
5. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program

12. Definitions and Acronyms

CO – Crypto Officer

CU – Crypto User

HSM – Hardware Security Module

KBK – Key Backup Key

KLK – Key Loading Key

KAT – Known Answer Test