FIPS 140-2 Level 3 Non-Proprietary Security Policy

NITROX XL 1600-NFBE HSM Family

Document number: CN16xx-NFBE-SPD-L3
Document Version: Version 3.5
Revision Date: 8/21/2018

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 CMVP lab comments
0.4.4	12/13/2009	Prasad Vellanki	Incorporated comments from CMVP Lab
1.0	1/14/2010	Prasad Vellanki	Final Changes
1.1	6/11/2010	Prasad Vellanki	Incorporated comments from CMVP Lab
2.0	1/12/2011	Mike Scruggs	Added changes relative to firmware version 2.0 from firmware version 1.x
2.1	9/06/2011	Ahmed Khan	Added 2.1 Firmware changes relative to 2.0
2.1- Bld16	8/26/2013	Ram Kumar	2.1 Build 16 specific changes
2.2	9/15/2014	Phanikumar	FW-2.2 build 130007 specific changes. Added support for TLS 1.1 and TLS 1.2. Added AES GCM, ECB. Handled SP 800-131A transition requirements.
2.3	12/03/2014	Phanikumar	Firmware version updated to CN16XX-NFBE-FW-2.2-130009. Minor changes in Section 6 to address CMVP comments.
2.4	12/23/2014	Phanikumar	Added hardware version descriptions in Section 1. Updated Table 16 for clarification.
2.5	1/7/2015	Phanikumar	Updated table 3
2.6	6/30/2015	Phanikumar Kancharla	Updated with SFF device part number and pictures
2.7	11/18/2015	Phanikumar Kancharla	Firmware version updated to CN16XX-NFBE-FW-2.2-130011
3.0	1/24/2018	Phanikumar Kancharla	FW-2.3 specific changes, include TDES, AES keywrap and RSA PSS
3.1	3/2/2018	Phanikumar Kancharla	Updated Figure 6, Table 2, Section 8.2, and related text.
3.2	5/24/2018	Phanikumar Kancharla	Updated per CMVP Comments
3.3	6/20/2018	Phanikumar Kancharla	Updated per CMVP Comments
3.4	6/29/2018	Phanikumar Kancharla	Updated per CMVP Comments
3.5	8/21/2018	Phanikumar Kancharla	Updated FW version due to bug fixes

Table of Contents

List of Tables

List of Figures

1 Module Overview

The Cavium Inc. 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 1.0/1.1/1.2 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 interface via an API defined by the module.

The module is a hardware/firmware multi-chip embedded cryptographic module. The module provides cryptographic primitives to accelerate approved and allowed algorithms for TLS 1.0/1.1/1.2 and SSH. This module itself does not perform SSH, but accelerates the algorithms. The cryptographic functionality includes modular exponentiation, random number generation, and hash processing, along with protocol specific complex instructions to support TLS 1.0/1.1/1.2 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.

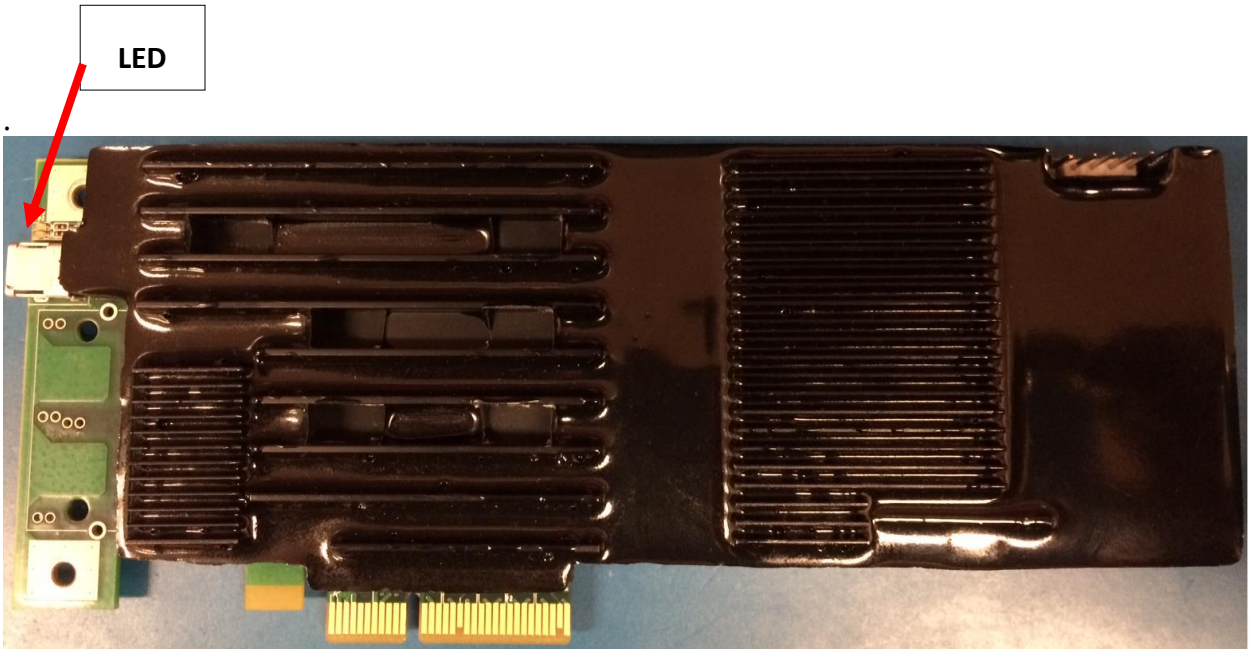

Figure 1 – Top View of NITROX XL 1600-NFBE HSM

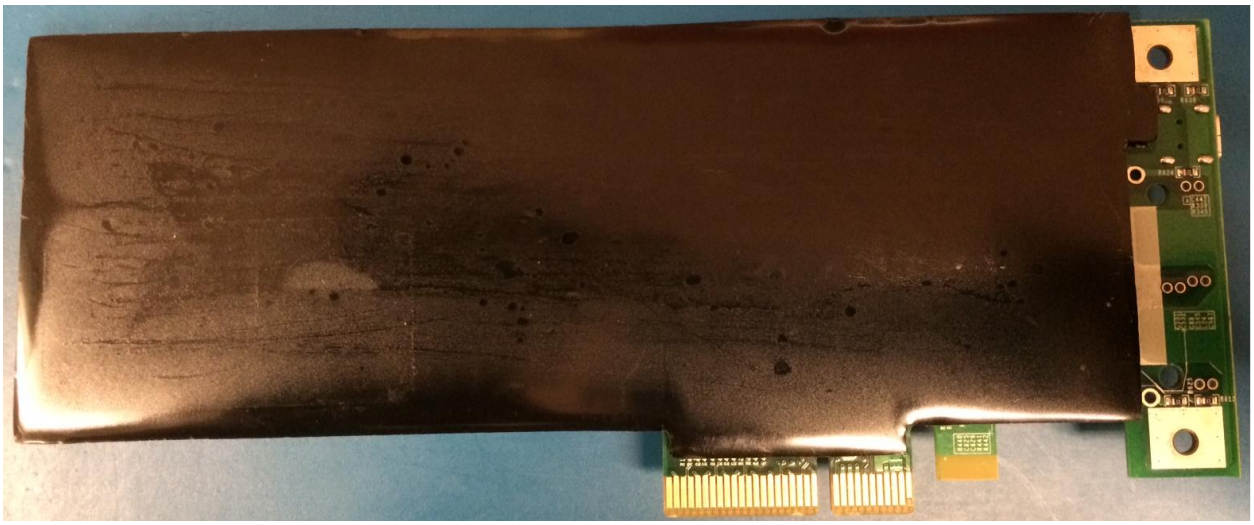

Figure 2 – Bottom view of NITROX XL 1600-NFBE HSM

Figure 3 - Top View of P/N FN1620-NFBE2-G

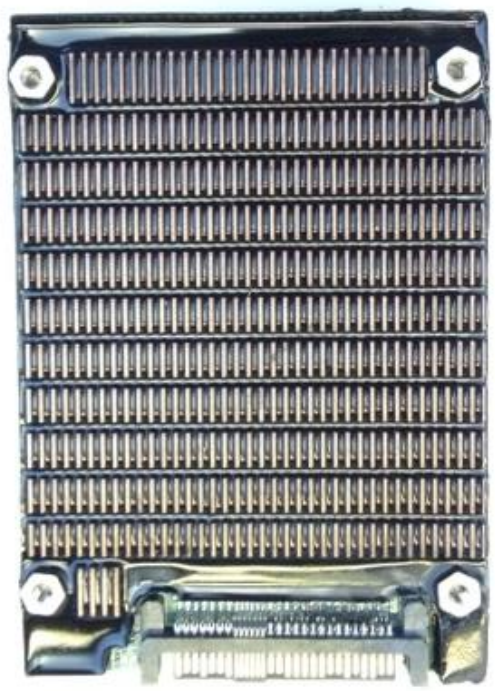

Figure 4. - Bottom View of P/N FN1620-NFBE2-G

The configuration of hardware and firmware for this validation is:

Hardware Part Numbers:

PCIe Half Size adapterversion

CN1610-NFBE1-3.0-G
CN1620-NFBE1-3.0-G
CN1620-NFBE3-3.0-G
CN1610-NFBE1-2.0-G
CN1620-NFBE1-2.0-G
CN1620-NFBE3-2.0-G

Small Form Factor version

FN1620-NFBE2-G

Firmware Version: CN16XX-NFBE-FW-2.3-180205 and
CN16XX-NFBE-FW-2.3-180821.

The three main hardware part numbers (CN1610-NFBE1, CN1620-NFBE1, and CN1620-NFBE3) differ only in performance capabilities and throughput. These performance capabilities are controlled by specific configurations set in the factory. There are no hardware differences.

The differences between the two hardware versions (2.0 and 3.0) are as follows:

- Potting manufacturer
- Memory density (512MB vs. 1GB)
- USB (standard vs. mini)
- Location of power supply components

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

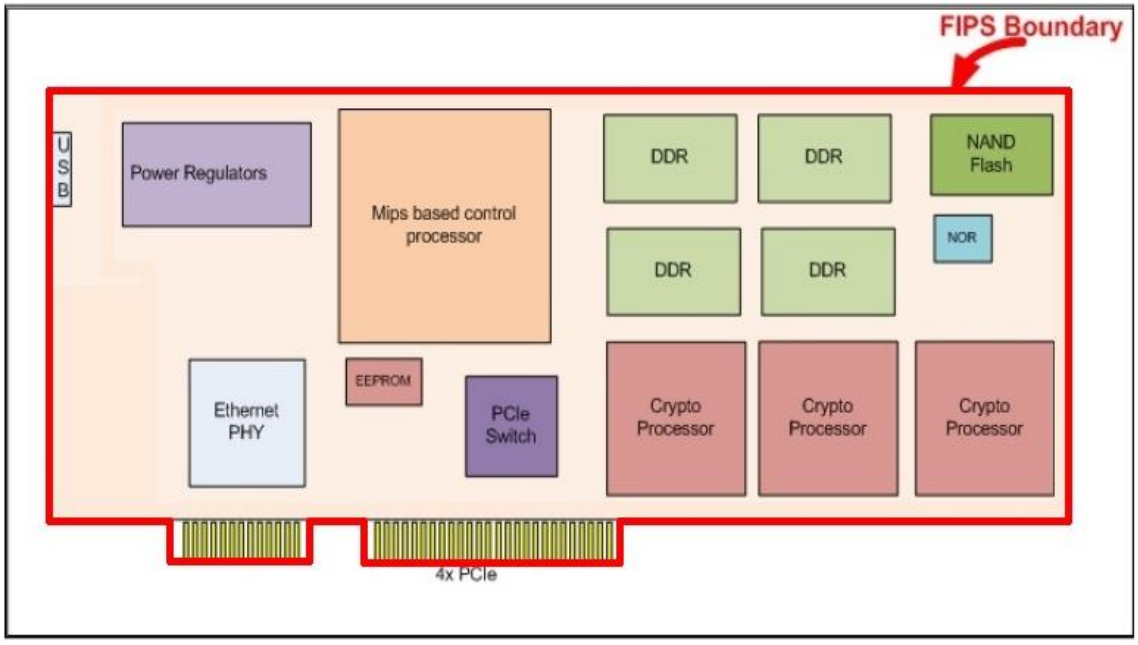

Figure 5 - FN1620-NFBE FIPS Boundary

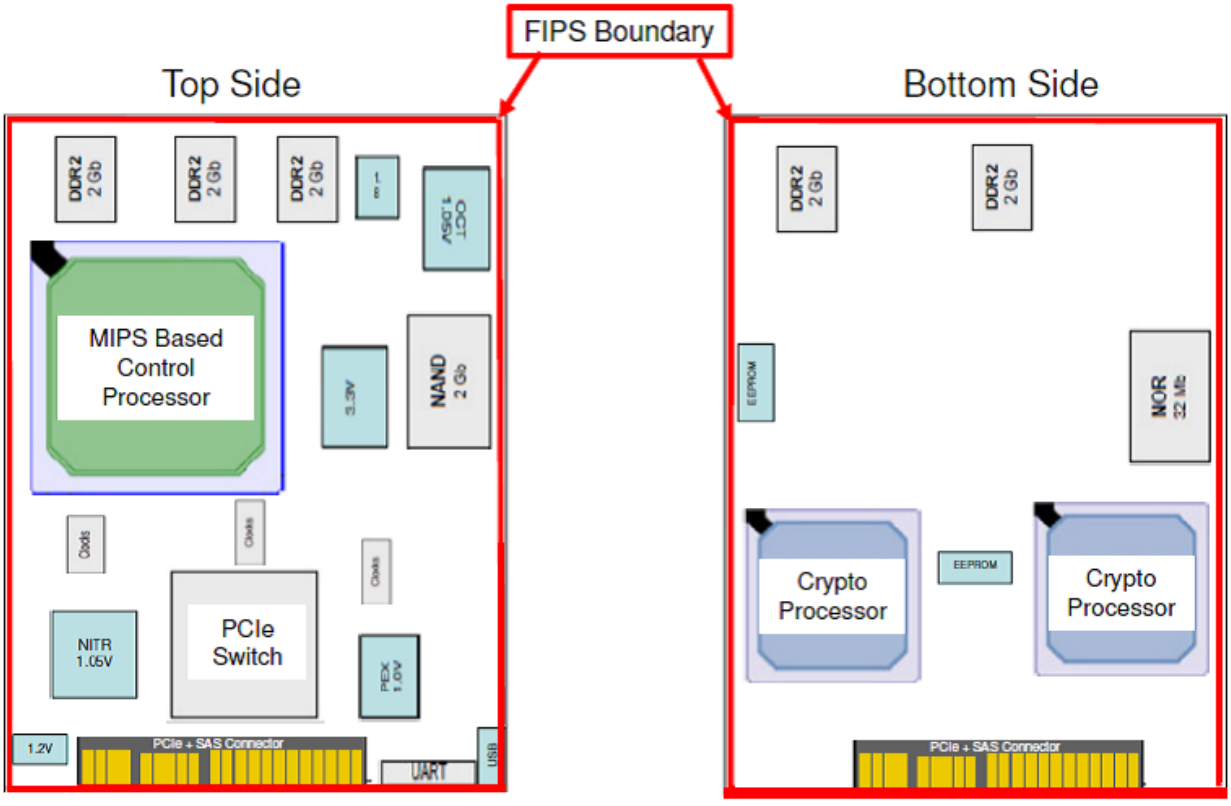

Figure 6: - FN1620-NFBE FIPS Boundary (Top and Bottom Side)

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. The following are the allowed values for fipsState parameters:

0 - Non-FIPS mode or zeroized state

2 - FIPS Approved mode with single factor authentication mechanism

3 - FIPS Approved mode with 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.

3.1 FIPS Approved Mode of Operation

The module provides a FIPS Approved mode of operation, comprising all services described in Section 6.1 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 Switching Modes

The Module Initilization Service configures the module, allowing it to operate in either the FIPS Approved Mode of Operation or the Non-FIPS Mode of Operation. This service is performed by a special Crypto Officer identity (the Default CO) which can only be accessed while in the zeroized state.

3.4 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	Cert.
AES: CBC; 128, 192, 256 bits	Data encryption and decryption	1265
AES: GCM*; 128, 192, and 256 bits AES-ECB has also been tested as a prerequisite to GCM.	Data encryption and decryption (AEAD)	2899
AES Key Wrap: 128, 192, 256 bits	Data encryption and decryption; Key Transportation (see KTS entry, below)	4026
CKG: SP800-133 §6: Aymmetric (FIPS 186-4, SP800-56A) §7: Symmetric (Direct output from DRBG) Note: The resulting symmetric key or generated seed is an unmodified output from a DRBG.	Key Generation	(Vendor Affirmed)
CVL: TLS KDF (v1.0/v1.1, v1.2)	Key Derivation for TLS	166
CVL: ECC-CDH (P-224, P-256, P-384, P-521)	Primitive with TLS exchange	847
DRBG: SP800-90A CTR DRBG using AES-256 (with DF)	Deterministic random bit generation	32
ECDSA KeyPair: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571 ECDSA PKV: All P, K and B curves ECDSA SigGen: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571 with SHA-224, SHA-256, SHA-384, SHA-512 ECDSA SigVer: All P, K and B curves with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Key Generation, public key validation and Signature Verification	1276
HMAC: SHA1: 160	Message integrity, authentication, TLS session key generation	443
HMAC: SHA2: 512	Message integrity, authentication	736
HMAC: SHA2: 256, 384 and 512	Message integrity, authentication, TLS session key generation	1677
KAS – SP800-56A (ECC; P-521)	Key agreement	153
KTS – SP800-38F	Key transport with AES-KW (256) Provides 256 bits of security strength.	4026 (AES)

FIPS Approved Algorithm	Usage	Cert.
	The module implements other forms of SP800-38F wrapping (AES-KW with 128, 192 bit keys; and Triple-DES TKW) but these are used only to wrap data.	
RSA KeyGen: 2048-bit and 3072-bit RSA SigGen (PKCS#1 v1.5, PSS): 2048, 3072, and 4096-bit with SHA-224, SHA-256, SHA-384, and SHA-512 RSA SigVer (PKCS#1 v1.5, PSS): 1024, 2048, 3072, and 4096-bit with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512	Key generation, Authentication and Signature Verification Note that RSA-4096 KeyGen is not testable due to CAVP tool limitations; it is allowed per IG A.14.	2701
SHA1:160	Secure hashing using Nitrox Px	801
SHA2:256, 384, 512	Secure hashing using Nitrox Px	1379
SHA1:160; SHA2: 256, 384, 512	For use during Signature generation and Verification in firmware.	1165
Triple-DES: CBC; 192 bits (3-key)	Data encryption and decryption	898
Triple-DES: ECB; 192 bits (3-key) Triple-DES Key Wrap	Data encryption and decryption	2204

* For GCM, the module falls under Category 4 of IG A.5. The Fixed Field of the IV is generated pseudorandomly by the TLS KDF, ensuring no other party encrypts using the same fixed field. The invocation field is provided by the operator; the operator provides invocation fields as part of a TLS implementation, which by its design prevents IVs from repeating. Note that the module does not perform all of TLS by itself (which is why this is under Category 4 rather than Category 1 of IG A.5). As a result, the operator must always invoke GCM with a "fresh" TLS session, and **not** re-use material from previous TLS sessions, modify keying material from a TLS handshake before use, or otherwise deviate from the normal usage of TLS.

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
MD5	Hashing within TLS KDF
Hardware RNG (NDRNG); provides 64 bits per access and is limited to instantiating the DRBG with 336 bits of security.	DRBG seed generation (512 bits total EI+Nonce)
RSA Key Wrap, non-compliant with SP800-56B: • RSA-2048 PKCS#1 (key wrapping; key establishment methodology provides 112 bits of encryption strength) • RSA-2048/3072/4096 OAEP (key wrapping; key establishment methodology provides between 112 and 128 bits of encryption strength) • RSA-1024 OAEP (legacy function; decryption only)	CSP Encrypt/Decrypt

The support of TLS 1.0/1.1/1.2 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 module operator as part of TLS protocol negotiation. (In general, no parts of TLS, other than the KDF, are tested by the CAVP or CMVP.)

3.5 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	Cert
RC4	Encryption/Decryption	RC4 key of 128 bits	N/A
PBE	Key generation	Password	N/A

3.6 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 (Hardware)	3
RSA Sig Ver	4
RSA Key Gen	5
RSA Enc/Dec	6
SHA 160 (Firmware)	10
HMAC SHA512 (Firmware)	11
DRBG (SP-800-90 KAT)	12
ECDSA Key Gen	13
ECDSA PKV	14
ECDSA Sig Ver	15
KAS (IG9.6) KAT	16
AES ECB (Encrypt, Decrypt Hardware for DRBG)	17
HMAC SHA1, SHA256, SHA512(Hardware)	18
AES ECB (Encrypt, Decrypt)	19
AES GCM (Encrypt, Decrypt)	20
DRBG continuous number test	12
ECDSA PKV Conditional Test	14
Hardware RNG continuous number test	24
ECDSA Pairwise Consistency Conditional Test	25

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
USB Interface	USB Interface USB0_DP, USB0_DM	Power No functionality in FIPS mode	USB Interface Not used in FIPS mode Physical connector varies based on form factor (type B, standard or mini)
Serial Interface	4 Pin serial interface - GND, 3.3V, Tx, Rx	N/A No functionality in FIPS mode	Disabled at the hardware level during the firmware load process.
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 Large form factor uses PCIe connector, small form factor uses SAS connector (U.2) instead.
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: Case In-Sensitive Username and 7 to 14 character encrypted password. Two factor: 1) Case In-Sensitive Username and 7 to 14 character encrypted password 2) An RSA 2048-bit signed challenge.
CU	This role has access to all crypto services offered by the module.	Identity-based operator authentication	Single factor: Case In-Sensitive Username and 7 to 14 character encrypted password. Two factor: 1) Case In-Sensitive Username and 7 to 14 character encrypted password 2) An RSA 2048-bit 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 seven (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

Note that the services listed in Tables 8-10 below are also available in the non-FIPS Approved mode (utilizing non-Approved algorithms).

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
Module Initialization	Put module into the approved mode and set up policies. This can only be run from a zeroized state. (This same process is used to put the module into non-approved mode, refer to Section 3.3 for details.)
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 MAC	Generates 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	Encrypts and decrypts data using keys in the module.
Show Status	Displays the status of the module like configuration, FIPS Approved mode, free memory, and used sessions. Fipsstate field indicates the mode of operation for the HSM.
Session Status	Shows the login status of the session.
Zeroize Module	Zeroizes all plaintext CSPs in the module by overwriting memory in all locations, delete users, clear policies, and return the module to a zeroized state.
Reset Module	Logical reset of the module. This service functions the same as a hardware reset, except that it does not reset host-side PCIe bus interface configuration.
Generate KLK	Generates KLK which can be used in importing a key into the module.
FW Upgrade	Upgrades to a new firmware image
FW Downgrade	Downgrades firmware image

6.1.2 CU services

Table 9 – Authenticated Services (CU only)

Service	Description
Key and Key Pair Management	Generates, imports, deletes and changes label of symmetric and asymmetric keys. Outputs plaintext public key.
Generate KLK	Generates KLK.

Secure Backup / Restore	Masks and unmasks symmetric and asymmetric keys using masking key in the module.
Encrypt/Decrypt Data	Encrypts and decrypts data using keys in the module.
Sign/Verify Data	Generates signature on given data and verifies a pre-generated signature.
Wrap/Unwrap data	Performs SP 800-38F wrap or unwrap of given databuf.
Secure Key Load	Enters CSPs into the module in encrypted form.
Generate MAC	Generates a message authentication code using HMAC.
Generate Random Number	Generates FIPS approved random number of given size.
Change CU Password	Changes CU password.
Logout	Logs out the operator (returns the module to the unauthenticated state) and closes the session.
Show Status	Displays the status of the module like configuration, FIPS Approved mode, free memory, and used sessions. Fipsstate field indicates the mode of operation for the HSM.
Session Status	Shows the login status of the session.
Zeroize Module	Zeroizes all plaintext CSPs in the module by overwriting memory in all locations, delete users, clear policies, and return the module to a zeroized state.
Reset Module	Logical reset of the module. This service functions the same as a hardware reset, except that it does not reset host-side PCIe bus interface configuration.
TLS Handshake	Run TLS handsahek with RSA and/or ECDH key exchange, establish TLS Session Keys in onbard context memory.
TLS Record Processing	Encrypt and decrypt the TLS records using the TLS Session Keys in context.

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	Displays the status of the module like configuration, FIPS Approved mode, free memory, and used sessions. Fipsstate field indicates the mode of operation for the HSM.
Session Status	Shows 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, delete users, clear policies, and return the module to a zeroized state.
Reset Module	Logical reset of the module. This service functions the same as a hardware reset, except that it does not reset host-side PCIe bus interface configuration. When powering back up, the power-up self-tests will run.

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 (which uses a physical PCIe port or an SAS port, depending on form factor).

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
Module Initialization	Session handle	Policies including approved or non-approved mode, user credentials	N/A	SUCCESS/FAILURE
Reset Module	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
Sign/Verify Data	Session handle	Plain Data/Signature, Key handle	Signature/Status	SUCCESS/FAILURE
Wrap/Unwrap Data	Session handle	Plain/Wrapped Data, Key handle	Wrapped/Unwrapped data	SUCCESS/FAILURE
Encrypt/Decrypt Data	Session handle	Plain/Encrypted Data, Key handle	Encrypted/Decrypted 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
Generate Random Number	Session handle	Size	Random 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
FW Upgrade	Session Handle	New FW image	N/A	SUCCESS/FAILURE
FW Downgrade	Session Handle	New FW image	N/A	SUCCESS/FAILURE

Service	Control Input	Data Input	Data Output	Status Output
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
TLS Handshake	Session Handle	TLS peer parameters, Private Key handle, Context handle.	Encrypted or plain text Client and Server Finished messages	SUCCESS/FAILURE
TLS Record Processing	Session Handle	TLS record data, Context handle	Plain or Encrypted TLS record.	SUCCSES/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 operator Login Public Keys for Crypto User (CU) and Crypto-Officer (CO) are generated on a 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
DRBG EI & Seed	Entropy Input & Seed	Entropy Input and seed for CTR_DRBG, taken from NDRNG (length varies)
DRBG State	CTR_DRBG Internal state	V (128 bits) and Key (256 bits) internal state values for CTR_DRBG
Master Key	AES-256 key	Used to encrypt and decrypt a subset of CSPs stored in the module.
KBK (Key Backup Key, aka Masking Key)	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 ECC Private Key	512 bit ECDSA Private key	Used for key agreement in the Clone Masking Key service. (Public key: Cloning ECC {Initiator, Responder} Public Key)
Cloning RSA	4096 bit RSA Private	Used for key agreement in the Clone Masking Key service.

Key Name	Type	Description
Private Key	Key	(Public key: Cloning RSA {Initiator, Responder} Public Key)
Cloning Shared Secret (Z)	Random number	Output from the Approved KDF.
Clone Session Encryption Key	AES-256 key	Ephemeral wrapping key generated as part of key agreement scheme. This key is used for wrapping of the Key Backup Key (KBK) during module masking key service.
Key Loading ECC Private Key	P-521 bit ECDSA Private key	Used for key agreement of key import service to derive KLK. (Public key: Key Load ECC {Initiator, Responder} Public Key)
Key Loading RSA Private Key	4096 bit RSA Private Key	Used for key agreement of key import service to derive KLK. (Public key: Key Load RSA {Initiator, Responder} Public Key)
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 also 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 also compared during the Login service to authenticate the CO.
PSWD_DEC Private Key	2048-bits RSA private key	Used to decrypt the operator supplied encrypted password during user creation and login. (Public key: Password Encryption Public Key)
RSA Private Key	RSA key of 2048 to 3072 bits	Generated, imported, or inserted into the module using the module services.
ECC or ECDSA Private Key	ECC key of curves P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571	Generated, imported, or inserted into the module using the module services.
Triple-DES Symmetric Keys	Triple DES 192 bit Key	Generated, 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 DRBG. If transported or entered, the module uses the KLK.
AES Symmetric Keys	Set of AES-128, 192, 256 keys	Generated, 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 DRBG. If transported or entered, the module uses the KLK.
HMAC-SHA Key	Random number	Secret key used to generate HMAC-SHA MAC data.
TLS KDF States	KDF Internal	TLS Pre-Master Secret (size varies) and TLS Master Secret (384 bits); used to generate TLS session keys (see below)
TLS 1.0/1.1/1.2 Session AES Symmetric Key	AES 128, 256	Generated as part of the TLS 1.0/1.1/1.2 protocol negotiation.
TLS 1.0/1.1/1.2 Session Triple-DES Symmetric Key	Triple DES 192	Generated as part of the TLS 1.0/1.1/1.2 protocol negotiation.

Key Name	Type	Description
TLS 1.0/1.1/1.2 Session MAC Key	HMAC-SHA-1/SHA-2 key	Generated as part of the TLS 1.0/1.1/1.2 protocol negotiation.
Clone Session MAC Key	HMAC-SHA-256 key	Generated as part of key agreement scheme and used as key confirmation during clone masking key service.
PAC	Password/ Authentication Info	Imported as part of the EAP-FAST authentication.

6.3 Definition of Public Keys

The module contains the following public keys:

Table 13 – Public Keys

Key Name	Type	Description
Password Encryption Public Key	2048 bits RSA public key	Used by operator to encrypt the user passwords during user creation and login. The encrypted passwords will be decrypted by the associated PSWD_DEC Private Key
Cloning Initiator ECC Public Key	ECC Static public key (P-521)	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 ECC Public Key	ECC Static public key (P-521)	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 ECC Public Key	ECC Static public key (P-521)	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 ECC Public Key	ECC Static public key (P-521)	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).
Cloning Initiator RSA Public Key	4096 bit Static RSA Public Key	Used in RSA encryption/decryption exchange to generate shared secret Z. At HSM level, used to establish secure channel for cloning process (to export Masking Key).
Cloning Responder RSA Public Key	4096 bit Static RSA Public Key	Used in RSA encryption/decryption exchange to generate shared secret Z. At HSM level, used to establish secure channel for cloning process (to export Masking Key).
Key Load Initiator RSA Public Key	4096 bit Static RSA Public Key	Used in RSA encryption/decryption exchange to generate shared secret Z. At HSM level, used to establish secure channel for cloning process (Secure Key Loading).
Key Load Responder RSA Public Key	4096 bit Static RSA Public Key	Used in RSA encryption/decryption exchange to generate shared secret Z. At HSM level, used to establish secure channel for cloning process (Secure Key Loading).
CO Login Public Key	2048 bit 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	2048 bit RSA public key	Used for signature verification in a challenge / response protocol during Login process as an optional second authentication factor.

Key Name	Type	Description
Cloning ECC Domain Parameter Set	ECC P-521 curve domain parameters	Domain parameter set D (Set EE) ECC P-521 curve domain parameters used in SP 800-56A C(0,2,ECC DH) key agreement to deriveshared secret Z.
User Generated Public Keys	RSA:1024 to 3072. ECDSA: All NIST supported curves, Appendix A.	All Keys are used for signature verification. Note that certain keys must only be used for legacy operations. (RSA <2048, DSA-1024, ECC <224; refer to SP800-131A for details.)
FW Validation Key	2048 bit RSA public key	Authenticates FW images loaded into the module.
License Key	2048 bit RSA public key	RSA 2048-bit public key certificate used to validate the license service for module configuration

6.4 Definition of Session Key

The cryptographic module supports the generation/import/export of user keys which are bound to a session and are termed as session keys. Following points apply to the session keys:

- Session keys are stored in RAM and are lost across reboots.
- Session key access is restricted to an application in which it is created.
- Every session in an application will have access to the key's created by every other session in the same application.
- When a session is closed, the session keys created by that session get destroyed.

The module contains the following session keys:

Table 14 – Session Keys

Key Name	Type	Description
User Generated Public Keys	RSA: 1024 to 4096 bits in intervals of 256 bits. ECDSA: All NIST supported curves, Appendix A and B.	Keys are used for signature verification. Note that certain keys must only be used for legacy operations. (RSA <2048 ECC <224; refer to SP800-131A for details.)
RSA Private Keys	RSA key of 2048 to 4096 bits	Generated, imported, or inserted into the module using the module services.
ECDSA Private Key	NIST supported curves listed in Appendix A.	Generated, imported, or inserted into the module using the module services.
Triple-DES Symmetric Keys	Set of Triple-DES-192 keys	Generated, 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 DRBG. If transported or entered, the module uses key transport of 256 bits of strength.
AES Symmetric Keys	Set of AES-128, 192, 256 keys	Generated, 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 DRBG. If transported or entered, the module uses key transport of 256 bits of strength.

6.5 Definition of CSPs Modes of Access

Table 16 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 15 – 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	Module initialization	W, G	G: Password Encryption Keypair (PSWD_DEC

Role	Service	Mode	Cryptographic Key or CSP
			Private Key, Password Encryption Public Key), DRBG EI & Seed, DRBG State, Master Key, Cloning Initiator Public Keys, KBK, Cloning Initiator Private Keys W: CO Password, CU Password, PAC
Unauthenticated	Reset Module	Z, G	Z: All keys in temporary memory (RAM)* G: DRBG EI & Seed, DRBG State
CO	Clone Masking Key	G, R, Z	R: Cloning Initiator Public Key, Cloning Responder Public Key, Cloning Private Key, KBK, Masking Key GRZ: Cloning Shared Secret, Clone Session Encryption Key, Clone Session MAC Key
CO	Performance Configuration	None	None
CO	Generate MAC	R	HMAC-SHA Key
CO	Change CO Password	R	Password Encryption public Key, Crypto User Password, Crypto Officer Password
CO	Logout	None	None
CO	Encrypt/Decrypt Data	R	R: AES Symmetric Keys, Triple-DES Symmetric Keys, User Generated Public Keys
CO	Show Status	None	None
CO	Session Status	None	None
CO	Zeroize Module	Z	All CSPs
CO	Reset Module	Z	All keys in temporary memory (RAM)*
CO	Generate KLK	G, R, W, Z	R: Key Load Initiator Public Key W:Key Load Responder Public Key G, Z: Key Load Initiator Public Key, Key Load Initiator Private Key, Key Loading Private Key, Key Loading Shared Secret, Key Loading Key
CO	FW Upgrade	W	W: FW Validation Key, License Key
CO	FW Downgrade	W	W: FW Validation Key, License Key
CU	Key and Key Pair Management	G, R, W, Z	R: KLK G, R, W, Z: AES Symmetric Keys, Triple-DES Symmetric Keys, HMAC-SHA Key, RSA Private Keys, User Generated Public Keys, Password Encryption public key(RSA)
CU	Generate KLK	G, R	R: Key Load Initiator Public Key, Masking Key W:Key Load Responder Public Key G, Z: Key Load Initiator Public Key, Key Load Initiator Private Key, Key Loading Private Key, Key Loading Shared Secret, Key Loading Key

Role	Service	Mode	Cryptographic Key or CSP
CU	Secure Backup/Restore	G, R, Z, W	R: KBK, GRZ:Symmetric Key/Asymmetric Key RW: RSA Private Key, RSA Private Session Key, User Generated Public Keys, 3_DES Symmetric Key, 3_DES Symmetric Session Key, ECDSA Private Key, ECDSA Private Session Key, AES Symmetric Key, AES Symmetric Session Key, HMAC-SHA Key
CU	Encrypt/Decrypt Data	R	R: AES Symmetric Keys, Triple-DES Symmetric Keys, User Generated Public Keys
CU	Sign/Verify Data	R	R: RSA Private Key, User Generated Public Keys
CU	Wrap/Unwrap Data	R	R: AES Symmetric Keys, Triple-DES Symmetric Keys
CU	Secure Key Load	G, R, W	R: Key Load Initiator Public Key, Key Load Responder Public Key, Key Load private key, GR: Key Loading Key W: RSA Private Key, RSA Private Session Key, User Generated Public Keys, 3_DES Symmetric Key, 3_DES Symmetric Session Key, ECDSA Private Key, ECDSA Private Session Key, AES Symmetric Key, AES Symmetric Session Key, HMAC-SHA Key
CU	Generate MAC	R	R: HMAC-SHA Key
CU	Generate Random Number	R	R: DRBG State G: RSA Private Key, RSA Private Session Key User Generated Public Keys, 3_DES Symmetric Key, 3_DES Symmetric Session Key, ECDSA Private Key, ECDSA Private Session Key, AES Symmetric Key, AES Symmetric Session Key, HMAC-SHA Key
CU	Change CU Password	W	W: Password Encryption public Key, Crypto User Password, Crypto Officer Password
CU	Logout	None	None
CU	Show Status	None	None
CU	Session Status	None	None
CU	Zeroize Module	Z	Z: All CSPs
CU	Reset Module	Z, G	Z: All keys in temporary memory (RAM)* G: DRBG EI & Seed, DRBG State
CU	TLS Handshake	R, G	R: RSA/ECC keys G: TLS KDF States, TLS Session keys
CU	TLS Record Processing	R	R: TLS Session keys

* The following keys are stored in RAM:

Cloning Responder Public Key, TLS Session Keys, Cloning Session MAC Key, AES Symmetric Session Key, ECDSA Private Session Key, 3_DES Symmetric Session Key, RSA Private Session Key, KeyLoading Shared Secret (Z), Cloning Shared Secret (Z), Cloning Session Key, CTR_DRBG internal State

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 & Guidance

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

8.1 Procedural

While this Level 3 module enforces most rules on its own (see "Automatic", below), there are a few exceptions:

1. The module must be configured for FIPS operation by following the first-time initialization procedure described in Section 4 of the User Manual and C-API Specification (CN16xx-NFBE-API-0.9: https://support.cavium.com/websilo/document/JmlfaWQ9Nzc2OCZwX2lkPTMzNwA)
    a. Provide the default CO pin
    b. Provide the HSM label
    c. Set the FIPS mode flag to TRUE for FIPS 140-2 Level 3
2. The operator must not misuse AES-GCM. Refer to the note under Table 3 for details.
3. The user must restrict their usage of legacy algorithms to appropriate "legacy" situations, such as the verification of data signed using a SHA-1 hash before it was disallowed by SP800-131A. No module can enforce this when the context is external (i.e. when the module provides an algorithm to the operator for arbitrary external use). The following algorithms within the module are for legacy use only:
    a. All signature verification operations with SHA-1 as the hash (RSA, ECDSA)
    b. ECDSA verification operations with curves smaller than 224 (see Appendix B of this document).
    c. RSA verification or decryption operations with key sizes smaller than 2048 (e.g. RSA-1024).
4. The user must restrict the use of Triple-DES as per FIPS IG §A.13. A Triple-DES key must not be used for more than 2^{20} encryption operations (roughly 8.38MB) for IETF protocols, such as TLS (Per RFC's 2246, 4346, 5246), or 2^{16} encryption operations (roughly 524kB) for other use-cases. (This provision is subject to change; please refer to NIST.gov for the current restrictions.) This is allowed to be procedural at Level 3 as per IG A.13.
5. Any new software/firmware loaded onto the module must be covered by a FIPS 140-2 validation certificate in order for this device to remain a FIPS module.

8.2 Automatic

The following security rules are enforced by the module automatically. No operator action is required.

1. The cryptographic module clears previous authentications on power cycle
2. When the module has not been placed in a valid role, the operator does not have access to any security-relevant services.
3. The cryptographic module performs the following power up, continuous and conditional self-tests
   A. Power-Up Tests
   - AES-128 CBC Encrypt & Decrypt KATs (Cert. #1265)
   - AES-256 ECB Encrypt & Decrypt KATs (Cert. #1265)

- AES-128 ECB, GCM Encrypt & Decrypt KATs (Cert. #2899)
- AES-256 key wrap/unwrap KATs (Cert. #4026)
- DRBG KAT (Cert. #32)

- ECDSA (all curves) Sig Gen/Ver, KeyGen and PKV KATs (Cert. #1276)
- HMAC-SHA-1, SHA-256, ad SHA-512 KATs (Certs. #443, #1677) (Covers SHS #801, #1379)
- HMAC-SHA-512 KAT (Cert. #736) (Covers SHS #1165)
- SHS KAT 160 bit (Cert. #801)
- SHS KAT 160 (Cert. #1165)
- RSA-2048/3072 Sig Gen/Ver with (SHA-1 [verify only], SHA-256, SHA-384, and SHA-512) KATs (Cert. #2701) (Covers SHS #1165, #1166)
- RSA Encrypt & Decrypt KATs
- KAS KAT per IG 9.6 (Q=dG and KDF)
- Firmware integrity test (CRC16)
- Triple-DES Encrypt & Decrypt KATs (Cert. #898)
- Triple-DES key wrap/unwrap KATs (Cert. #2204)

B. Conditional Self-Tests

- ECDSA Pairwise Consistency Test
- RSA Pairwise Consistency Test
- SP800-90A CTR_DRBG Continuous number test
- KAS conditional test
- HW RNG Continuous Number Test
- FW Load test (RSA-2048)

4. Critical Functions Tests: The module runs the 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 can command 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 is 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 zeroization services zeroizes all keys and other CSPs, without restriction.
10. The module does not support a maintenance interface or role.
11. The module does not support bypass capabilities.
12. The module does not support manual key entry.
13. The module has no CSP feedback to operators.
14. The module does not enter or output plaintext CSPs
15. The module does not output intermediate key values.

9 Physical Security Policy

9.1 Physical Security Mechanisms

For all variants, the module's cryptographic boundary is defined to be the outer perimeter of the hard epoxy enclosure containing the hardware and firmware 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.

Note: Module hardness testing was only performed at ambient temperature. No assurance is provided for Level 3 hardness conformance at any other temperature.

10 Mitigation of Other Attacks Policy

No mitigation of other attacks are implemented by the module.

11 References

1. NIST Special Publication SP800-38F, December, 2012.
2. NIST Special Publication 800-56A, March, 2007.
3. NIST Special Publication 800-56B, August, 2009.
4. NIST Special Publication 800-57 Part-1, May 2006.
5. FIPS PUB 140-2, FIPS Publication 140-2 *Security Requirements for Cryptographic Modules*
6. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program

12 Definitions and Acronyms

CO – Crypto Officer

CU – Crypto User

ECC – Elliptic Curve Cryptography

HSM – Hardware Security Module

KBK – Key Backup Key

KLK – Key Loading Key

KAT – Known Answer Test

Appendix A: Supported ECC curves

Curves over prime number fields: P-224, P-256, P384, P-521.

Koblitz curves over 2^m fields: K-233, K-283, K-409, K-571.

Curves over 2^m fields: B-233, B-283, B-409, B-571.

Appendix B: Limited usage ECC curves (SP 800-131A)

Curves over prime number fields: P-192

Koblitz curves over 2^m fields: K-163

Curves over 2^m fields: B-163