FIPS 140-2 Level 3
Non-Proprietary Security Policy

NITROXIII CNN35XX-NFBE HSM Family

Document number: CNN35xx-NFBE-SPD-L3
Document Version: Version 2.06.17
Revision Date: 6/21/2023

Revision History

Revision	Date	Author	Description of Change
2.06.02	11/12/2019	Phanikumar Kancharla	FW 2.06 build 03 CMVP Submission
2.06.03	6/4/2020	Phanikumar Kancharla	FW 2.06 build 05 with backward compatibility and input sanity bug fixes
2.06.04	9/17/2020	Phanikumar Kancharla	Updated Section 3, Table 4, and Table 5 in response to CMVP Comments
2.06.05	10/23/2020	Phanikumar Kancharla	FW 2.06 build 6 to address bug fixes; Table 4 updated to add CVL Cert. #C839
2.06.06	1/6/2021	Phanikumar Kancharla	FW 2.06 build 7 to address bug fixes
2.06.07	1/28/2021	Ruchitha Uppuluri	Updated Table 2 with new HW part numbers; minor reformatting
2.06.14	11/4/2021	Rajendar Kalwa	FW 2.06 build 14 to incorporate transition algorithm certs and bug fixes
2.06.15	3/21/2022	Rajendar Kalwa	Updated KAS certificate description in Table 4
2.06.15a	4/14/2022	Rajendar Kalwa	FW 2.06 build 15 for input sanity bug fixes
2.06.15b	5/3/2022	Rajendar Kalwa	Corrected HW versions in Table 2
2.06.16	10/7/2022	Rajendar Kalwa	Enhanced error handling and corresponding cleanup.
2.06-17	6/21/2023	Rajendar Kalwa	FW 2.06 build 17 for CVE fix and input sanity bug fix

Table of Contents

List of Tables

List of Figures

1 Module Overview

The NITROXIII CNN35XX-NFBE HSM Family module (hereafter referred to as *the module or HSM*) by Marvell (formerly Cavium Inc.) 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. 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 NITROXIII chip. The module implements password based single factor authentication at FIPS 140-2 Level 3 security. The physical boundary of the module is the outer perimeter of the card itself.

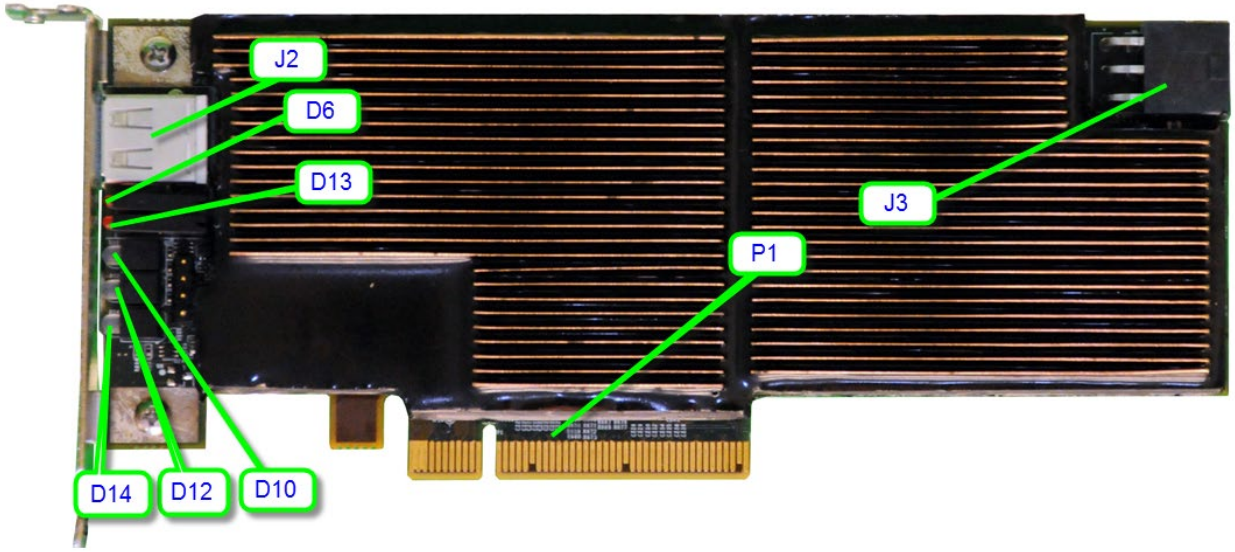

Figure 1 – Top View of Cryptographic Module

Table 1 – LED Description

LED Location	LED Description
D6 – Red	Power Fail indication
D6 – Green	Power OK – All voltages rails are at nominal
D13 – Red	See Table 7
D13 – Green	See Table 7
D10 –Multicolor	See Table 7
D12 – Multicolor	See Table 7
D14 – Multicolor	See Table 7

The configuration of hardware and firmware for this validation is:

Table 2 – Hardware Part Numbers

Part Number	HW Version	LiquidSecurity Appliance	Cores Enabled	Key Store Size	Max Partitions
CNL3560P-NFBE-G	HW-1.0	Yes	64	100K	32
CNL3560-NFBE-G	HW-1.0	Yes	64	100K	32
CNL3530-NFBE-G	HW-1.0	Yes	32	25K	32
CNL3510-NFBE-G	HW-1.0	Yes	24	25K	24
CNL3510P-NFBE-G	HW-1.0	Yes	32	50K	32
CNL3560P-NFBE-2.0-G	HW-2.0	Yes	64	100K	32
CNL3560-NFBE-2.0-G	HW-2.0	Yes	64	100K	32
CNL3530-NFBE-2.0-G	HW-2.0	Yes	32	25K	32
CNL3510-NFBE-2.0-G	HW-2.0	Yes	24	25K	24
CNL3510P-NFBE-2.0-G	HW-2.0	Yes	32	50K	32
CNL3560PB-NFBE-2.0-G	HW-2.0	Yes	64	100K	32
CNL3560B-NFBE-2.0-G	HW-2.0	Yes	64	100K	32
CNL3530B-NFBE-2.0-G	HW-2.0	Yes	32	25K	32
CNL3510B-NFBE-2.0-G	HW-2.0	Yes	24	25K	24
CNL3510PB-NFBE-2.0-G	HW-2.0	Yes	32	50K	32
CNL3560P-NFBE-3.0-G	HW-3.0	Yes	64	100K	32
CNL3560B-NFBE-3.0-G	HW-3.0	Yes	64	100K	32
CNL3560-NFBE-3.0-G	HW-3.0	Yes	64	100K	32
CNL3560A-NFBE-3.0-G	HW-3.0	Yes	64	100K	32
CNL3560C-NFBE-3.0-G	HW-3.0	Yes	64	100K	32
CNL3560D-NFBE-3.0-G	HW-3.0	Yes	64	100K	32
CNL3560E-NFBE-3.0-G	HW-3.0	Yes	64	100K	32
CNL3560F-NFBE-3.0-G	HW-3.0	Yes	64	100K	32
CNL3530-NFBE-3.0-G	HW-3.0	Yes	32	25K	32
CNL3530B-NFBE-3.0-G	HW-3.0	Yes	32	25K	32
CNL3530A-NFBE-3.0-G	HW-3.0	Yes	32	25K	32
CNL3530C-NFBE-3.0-G	HW-3.0	Yes	32	25K	32
CNL3530D-NFBE-3.0-G	HW-3.0	Yes	32	25K	32
CNL3530E-NFBE-3.0-G	HW-3.0	Yes	32	25K	32
CNL3530F-NFBE-3.0-G	HW-3.0	Yes	32	25K	32
CNL3510-NFBE-3.0-G	HW-3.0	Yes	24	25K	24
CNL3510P-NFBE-3.0-G	HW-3.0	Yes	32	50K	32
CNL3510A-NFBE-3.0-G	HW-3.0	Yes	32	50K	32
CNL3510C-NFBE-3.0-G	HW-3.0	Yes	32	50K	32
CNL3510D-NFBE-3.0-G	HW-3.0	Yes	32	50K	32
CNL3510E-NFBE-3.0-G	HW-3.0	Yes	32	50K	32
CNL3510F-NFBE-3.0-G	HW-3.0	Yes	32	50K	32
CNL3510I-NFBE-3.0-G	HW-3.0	Yes	24	25K	16
CNL3530I-NFBE-3.0-G	HW-3.0	Yes	32	25K	32
CNL3560I-NFBE-3.0-G	HW-3.0	Yes	64	100K	32
CNN3560P-NFBE-G	HW-1.0	No	64	100K	64
CNN3560-NFBE-G	HW-1.0	No	64	100K	32
CNN3530-NFBE-G	HW-1.0	No	32	25K	32

CNN3510-NFBE-G	HW-1.0	No	24	25K	24
CNN3510LP-NFBE-2.0-G	HW-2.0	No	24	25K	24
CNN3510LPB-NFBE-2.0-G	HW-2.0	No	24	25K	24
CNN3560P-NFBE-2.0-G	HW-2.0	No	64	100K	64
CNN3560P-NFBE-3.0-G	HW-3.0	No	64	100K	64
CNN3560-NFBE-2.0-G	HW-2.0	No	64	100K	32
CNN3560-NFBE-3.0-G	HW-3.0	No	64	100K	32
CNN3560A-NFBE-3.0-G	HW-3.0	No	64	100K	32
CNN3560C-NFBE-3.0-G	HW-3.0	No	64	100K	32
CNN3560D-NFBE-3.0-G	HW-3.0	No	64	100K	32
CNN3560E-NFBE-3.0-G	HW-3.0	No	64	100K	32
CNN3560F-NFBE-3.0-G	HW-3.0	No	64	100K	32
CNN3530-NFBE-2.0-G	HW-2.0	No	32	25K	32
CNN3530-NFBE-3.0-G	HW-3.0	No	32	25K	32
CNN3530A-NFBE-3.0-G	HW-3.0	No	32	25K	32
CNN3530C-NFBE-3.0-G	HW-3.0	No	32	25K	32
CNN3530D-NFBE-3.0-G	HW-3.0	No	32	25K	32
CNN3530E-NFBE-3.0-G	HW-3.0	No	32	25K	32
CNN3530F-NFBE-3.0-G	HW-3.0	No	32	25K	32
CNN3510-NFBE-2.0-G	HW-2.0	No	24	25K	24
CNN3510-NFBE-3.0-G	HW-3.0	No	24	25K	24
CNN3510A-NFBE-3.0-G	HW-3.0	No	24	25K	24
CNN3510C-NFBE-3.0-G	HW-3.0	No	24	25K	24
CNN3510D-NFBE-3.0-G	HW-3.0	No	24	25K	24
CNN3510E-NFBE-3.0-G	HW-3.0	No	24	25K	24
CNN3510F-NFBE-3.0-G	HW-3.0	No	24	25K	24
CNN3510LP-NFBE-3.0-G	HW-3.0	No	24	25K	24
CNN3510LPB-NFBE-3.0-G	HW-3.0	No	24	25K	24
CNN3510LPA-NFBE-3.0-G	HW-3.0	No	24	25K	24
CNN3510LPC-NFBE-3.0-G	HW-3.0	No	24	25K	24
CNN3510LPD-NFBE-3.0-G	HW-3.0	No	24	25K	24
CNN3510LPE-NFBE-3.0-G	HW-3.0	No	24	25K	24
CNN3510LPF-NFBE-3.0-G	HW-3.0	No	24	25K	24
CNN3505LP-NFBE-2.0-G	HW-2.0	No	16	10K	16
CNN3505LP-NFBE-3.0-G	HW-3.0	No	16	10K	16
CNN3505LPA-NFBE-3.0-G	HW-3.0	No	16	10K	16
CNN3505LPC-NFBE-3.0-G	HW-3.0	No	16	10K	16
CNN3505LPD-NFBE-3.0-G	HW-3.0	No	16	10K	16
CNN3505LPE-NFBE-3.0-G	HW-3.0	No	16	10K	16
CNN3505LPF-NFBE-3.0-G	HW-3.0	No	16	10K	16

LP is low-frequency part, where N3 chip runs at 500MHz, otherwise it runs at 600MHz.

CNN35XX-NFBE-G Firmware:

CNN35XX-NFBE-FW-2.06 build 17.

The module supports different performance options as 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. Also, the manufacturer can configure the HSM adapter to work only with Cavium's

LiquidSecurity HSM appliances, these parts are identified with CNL prefix. CNN cards can work with non-Cavium appliances. CNL and CNN part numbers employ the same hardware and firmware with the only difference being in vendor configuration where CNL parts require certificates in cloning service, which is optional in CNN.

The major blocks of the module are: General purpose MIPS based control processor, crypto processors, RAM memory, NOR and eMMC flash for persistent storage, USB interfaces, and PCIe gen-2 x8 interfaces.

2 Security Level

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

Table 3 – 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
Overall	3

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

2 - FIPS Approved mode with single factor authentication mechanism

3 - FIPS Approved mode with certificate based dual factor authentication mechanism

The indicator of Approved mode is obtained by using the Get Status service. The fipsState field of Get Status service indicates the mode. CSPs are not shared between the Approved and non-Approved modes of operation.

3.1 FIPS Approved Mode of Operation

The module provides a FIPS Approved mode of operation, comprising all services described in Section 7.3 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 6. All services are available in both the Approved and non-Approved modes of operation; however, the PCU Key Management and PCU Crypto Offload services are capable of employing non-FIPS Approved algorithms in the non-Approved mode.

3.3 Partitions

N3FIPS adapter is a sr-iov enabled intelligent PCIe adapter with 1 physical function and 128 virtual functions. In addition to the crypto offloads, this adapter can provide secure key storage with up to 64 partitions, including master partition. Each partition will have its own users to manage the partition and own configuration policies and hence each partition can be treated as a virtual HSM. HSM always has one default partition called HSM Master partition and this contains configuration of the complete HSM and default configuration of any additional partitions that are created. Only one HSM partition can be assigned to one SR-IOV virtual function of HSM adapter and vice-versa. Keys belonging to one partition are not accessible from other partition. This is achieved through a secure binding between partition and the PCIe virtual function.

3.3.1 HSM Master Partition

This is the default partition with only one user, called the Master Crypto Officer (MCO). This partition represents the operating state of the whole HSM adapter. i.e., initialization of HSM is nothing but initializing this partition with required configuration and MCO credentials. Zeroizing this partition will erase all HSM partitions in the adapter. The HSM has to be initialized and the MCO should already be logged in to create more partitions on the adapter. The MCO can backup and restore complete partition

including user data, partition configuration and user keys. All the backup data is encrypted with Backup keys.

3.3.2 HSM Partition

Each partition will have a different set of users to manage it and a dedicated key storage and crypto resources associated. A partition will have a default configuration supplied by the master partition and can be changed (within limits) during the partition initialization. When a partition is created by the MCO, it will be in a zeroized state and has to be initialized to do any keystore management or crypto function offloads. Partition initialization will create the Partition Crypto Officer (PCO). The PCO can later create up to 1024 users (PCO or PCU) on demand. Each user will have a unique user name to identify themselves. The User has to login to the partition/vHSM to issue any authorized commands. Users are authenticated using passwords submitted during the user creation.

4 Encrypted Communication Channels

The End to End encryption feature in the module allows an application to initiate an TLS connection with the firmware to ensure the confidentiality of the data communicated over PCIe path.

The connection is based on **TLS v1.2** with the cipher-suite **TLS_RSA_WITH_AES_128_GCM_SHA256** (known to OpenSSL as **AES128-GCM-SHA256**). The module will act as server, and host application will act as client. The **server private key** will be the partition private key PAK which is generated for each pHSM when the pHSM/partition is created. The **server certificate** used for the SSL connection is the partition certificate PAC. The complete chain will be validated by the host application (CavClient) before establishing the TLS connection.

The End to End encryption feature is enabled using the initialization configuration parameters. Once this feature is enabled, all commands except the initialize and open session are encrypted.

5 Supported Cryptographic Algorithms

This section provides the list of supported cryptographic algorithms segregated based on the operating mode.

5.1 Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithms.

Table 4 – FIPS Approved Algorithms Used in the Module

FIPS Approved Algorithm	Usage	Certificate
AES: – ECB mode: Encrypt/Decrypt; 128, 192 and 256-bit – CBC mode: Encrypt/Decrypt; 128, 192 and 256-bit – CTR mode: 128, 192 and 256-bit – XTS mode: 128 and 256-bit (Tested, but not used)	Data encryption and decryption	C839 (N3FIPS-NITROXIII-GC)
AES – CCM Mode: Encrypt/Decrypt; 128, 192 and 256-bit	Authenticated encryption and decryption	C839 (N3FIPS-NITROXIII-GC)
AES – CMAC Mode: MAC generate and verify; 128, 192 and 256-bit	Message authentication code generation and verification	C839 (N3FIPS-NITROXIII-GC)
AES: – GCM: Encrypt/Decrypt; 128, 192 and 256-bit – 96-bit random IV; TLS record encryption – GMAC is supported – IG A.5 Notes: – TLS 1.2 or other applications can offload GCM operations. – For TLS-1.2 protocol, IV constructed as described in RFC 5288. – IV is generated internally to the cryptographic module. – IV is not generated internally to the GCM algorithm boundary. – SP 800-38D §8.2.2 is used for GCM IV construction. – IVs are generated randomly, and IG A.5 Requirement #2 applies. – IV's free field is a 4-byte counter. – IV's random field is a 96-bit random number. – IV's random field is incremented by 1. IV's random field wouldn't overflow 96-bits in the lifetime of the module. – Internal Approved RNG: SP 800-90A DRBG, AES_CTR 256-bit or SHA-512. – Internal NDRNG used to seed the Approved RNG: Octeon HW random number generator	Data encryption, decryption, key-wrap and key-unwrap	C839 (N3FIPS-NITROXIII-GC)
AES: – ECB mode: Encrypt/Decrypt; 128, 192 and 256-bit – CBC mode: Encrypt/Decrypt; 128, 192 and 256-bit	Data encryption/decryption.	C819 (N3FIPS-OpenSSL-1.1.1-AES)

FIPS Approved Algorithm	Usage	Certificate
AES: – KW and KWP mode: Encrypt/Decrypt; 128, 192 and 256-bit	Key encryption/decryption.	C1263 (LiquidSecurity Keywrap)
CKG – IG D.12 – SP 800-133 Section 6.1 Asymmetric signature key generation using unmodified DRBG output – SP 800-133 Section 6.2 Asymmetric key establishment key generation using unmodified DRBG output – SP 800-133 Section 7.1 Direct symmetric key generation using unmodified DRBG output – SP 800-133 Section 7.3 Derivation of symmetric keys from a key agreement shared secret. – SP 800-133 Section 7.4 Derivation of symmetric keys from a pre-shared key	Key generation	N/A: Vendor Affirmed
CVL: SP 800-56A ECC CDH: P-224, P-256, P-384 and P-521	ECDH key derivation and SSL suite B key exchange	C829 (N3FIPS-NITROXIII-ECC)
CVL: FIPS 186-4 ECDSA SP: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, and B-571	ECDSA Signature generation on pre-hashed input messages	C825 (N3FIPS-OpenSSL-1.1.1-ECC)
CVL: – TLS-KDF (v1.0/1.1, v1.2)	TLS handshake	C840 (N3FIPS-NITROXIII-TLS-KDF)
CVL: - SP 800-56B RSADP - FIPS 186-4 RSASP1	RSA Decryption and Key Unwrap RSA Signature Primitive	C839 (N3FIPS-NITROXIII-GC)
CVL: – SP 800-56B RSADP	RSA Decryption Primitive	A1954 (OpenSSL)
DRBG: SP 800-90A DRBG: AES-CTR 256-bit	IV and nonce generation	680
DRBG: – SP 800-90A DRBG: AES-CTR 256-bit	Key generation	C821 (N3FIPS-OpenSSL-1.1.1-DRBG-CTR)
DRBG: – SP 800-90A DRBG: SHA512	Random number generation and key generation	C830 (N3FIPS-NITROXIII-DRBG-SHA)
DSA: – Key Gen: 2048 and 3072-bit – PQG Gen: 2048 and 3072-bit – PQG Ver: 1024-bit*, 2048 and 3072-bit – Sig Gen: 2048 and 3072-bit (SHA-224, -256, -384, -512) – Sig Ver: 1024*, 2048 and 3072-bit (SHA-1, 224, -256, -384, -512) * Legacy use only	Key generation, Sign and Verify	C823 (N3FIPS-OpenSSL-1.1.1-DSA)

FIPS Approved Algorithm	Usage	Certificate
ECDSA: – Key Gen: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, and B-571 – Key Ver: All P, K and B curves – Sig Gen and Sig Gen Component: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, and B-571 (SHA-224, -256, -384, -512) – SigVer: All P, K and B curves (SHA-1, 224, -256, -384, -512)	Key generation, Sign and Verify	C825 (N3FIPS-OpenSSL-1.1.1-ECC)
ECDSA: – Sig Gen Component: P-224, P-256, P-384, P-521 (SHA-224, -256, -384, -512) – SigVer: P-192, P-224, P-256, P-384, P-521 (SHA-1, 224, -256, -384, -512)	Signature generation and verification	C829 (N3FIPS-NITROXIII-ECC)
HMAC: HMAC-SHA-1, 224, 256, 384, 512	MAC generation and KAS	C822 (N3FIPS-OpenSSL-1.1.1-HMAC)
HMAC: – HMAC-SHA-1, 224, 256, 384, 512	MAC generation	C839 (N3FIPS-NITROXIII-GC)
KAS: – SP 800-56A rev3 KAS-ECC Ephemeral Unified with P-521 – One Step KDF – No key confirmation	Key Agreement for Cloning	A1952 (N3FIPS-KAS-ECC)
KAS-RSA: – SP 800-56B rev2 RSA/IFC based KAS using 2048-bit key size – 3072 and 4096-bit key sizes tested, but not used. – One Step KDF	Key Agreement	A1953 (OpenSSL)
KBKDF: – SP 800-108 HMAC-SHA-1, -224, -256, -384, -512 KDF – Counter mode	Key derivation	C826 (N3FIPS-OpenSSL-1.1.1-HMAC-KDF)
KBKDF: – SP 800-108 HMAC-SHA-256, 384, 512 KDF – SP 800-108 AES-CMAC 128-bit, 192-bit, and 256-bit – Counter mode	Key derivation	C839 (N3FIPS-NITROXIII-GC)
KDF: – ANSI X9.63 (SHA2-224, SHA2-256, SHA2-384, SHA2-512) (Tested, but not used)	Key derivation	C825 (N3FIPS-OpenSSL-1.1.1-ECC)
KTS – AES GCM provides between 128 and 256 bits of encryption strength	Key Transport	C839 (N3FIPS-NITROXIII-GC)
KTS – SP 800-38F AES KW and KWP, 128, 192 and 256-bit – SP 800-38F (AES) provides between 128 and 256 bits of encryption strength	Key Transport, Key wrap, unwrap, backup/restore	C1263 (LiquidSecurity Keywrap)

FIPS Approved Algorithm	Usage	Certificate
KTS – SP 800-38F (Triple-DES) provides 112-bits of encryption strength (limited to 2^16 encryption operations)	Key Transport	C1263 (LiquidSecurity Keywrap)
KTS-RSA – SP 800-56B rev2 RSA/IFC based KTS-OAEP using 2048, 3072, or 4096-bit key sizes. Provides between 112 and 150 bits of encryption strength. – SHA-224, SHA-256, SHA-384, SHA-512	Key wrap, unwrap	A1955 (N3FIPS-NITROXIII)
KTS-RSA – SP 800-56B rev2 RSA/IFC based KTS-OAEP using 2048, 3072, or 4096-bit key sizes. Provides between 112 and 150 bits of encryption strength. – SHA-224, SHA-256, SHA-384, SHA-512	Key wrap, unwrap	A1953 (OpenSSL)
RSA: – KeyGen: 2048, 3072-bit – FIPS 186-2 PKCS #1 1.5 and PSS SigGen: 4096-bit (SHA-224, -256, -384, -512) – FIPS 186-4 PKCS #1 1.5 and PSS SigGen: 2048 and 3072-bit (SHA-224, -256, -384, -512) – FIPS 186-4 PKCS #1 1.5 and PSS SigVer: 1024, 2048 and 3072-bit (SHA-1, 224, -256, -384, -512)	Key generation, Sign and Verify	C824 (N3FIPS-OpenSSL-1.1.1-RSA)
RSA: – KeyGen: 4096-bit – FIPS 186-4 PKCS #1 1.5 and PSS SigGen: 4096-bit (SHA-224, -256, -384, -512) – FIPS 186-4 PKCS #1 1.5 and PSS SigVer: 4096-bit (SHA-1, 224, -256, -384, -512)	Key generation, Sign and Verify	A1954 (OpenSSL)
SHS: SHA-1, 224, 256, 384 and 512	Data hashing	1780
SHS: – SHA-1, 224, 256, 384 and 512	Signature generation, verification, HMAC. SHA-1 used for verify only.	C820 (N3FIPS-OpenSSL-1.1.1-SHA)
Triple-DES (limited to 2^16 encryption operations): – TECB mode: 3-key Encrypt/Decrypt – TCBC mode: 3-key Encrypt/Decrypt	Data encryption and decryption	1311
Triple-DES (limited to 2^16 encryption operations): – TECB mode: 3-key Encrypt/Decrypt – TCBC mode: 3-key Encrypt/Decrypt	Data encryption and decryption Module limits Triple-DES encryptions to 2^16 64-bit blocks per IG A.13.	C1169 (N3FIPS-OpenSSL-1.1.1-TDES)
Triple-DES: – KW mode: 3-key Encrypt/Decrypt	Key encryption/decryption.	C1263 (LiquidSecurity Keywrap)

The cryptographic module supports the following non-FIPS Approved algorithms which are allowed for use in FIPS mode.

Table 5 – FIPS Allowed Algorithms Used in the Module

Algorithm	Usage
[IG D.9] AES: #C819 (N3FIPS-OpenSSL-1.1.1-AES) – ECB mode: Encrypt/Decrypt; 128, 192 and 256-bit – CBC mode: Encrypt/Decrypt; 128, 192 and 256-bit	Key unwrap only
[IG A.2] ECDSA Cert. #C829 and #C825, Secp256K1 (128 bits), X25519 (128 bits) (SHA-1*, SHA-224, SHA-256, SHA-384, SHA-512) *Legacy verification only	EC Key generation, Sign, Verify and ECDH.
[IG 7.15] Hardware RNG (NDRNG)	Seed, seed key generation
[IG D.9] RSA PKCS#1 of modulus size 2048, 3072 and 4096 bits (CVL Cert. #A1954, key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength).	CSP Encrypt/Decrypt
[IG D.9] RSA PKCS#1 of modulus size 2048, 3072 and 4096 bits (CVL Cert. #C839, key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength).	CSP Encrypt/Decrypt
[SP 800-135] MD5	Hashing within TLS

The support of TLS 1.0/1.1, v1.2 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 user of the module as part of TLS protocol negotiation. The TLS protocol has not been reviewed or tested by the CAVP or CMVP.

5.2 Non-Approved, Non-Allowed Algorithms

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

Table 6 – Non-Approved, Non-Allowed Algorithms Used in the Module

Algorithm	Usage	Keys/CSPs
PBE	Key generation	Password
ECDSA P192, EdCurve25519 (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)	Key generation, sign, and ECDH	EC Public and Private Key.

5.3 LED Error Pattern for FIPS Failure

On successful completion of the FIPS tests, the D10 Green 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. All blinks are 200ms ON and 200ms OFF. Blink delay time gap is 1000ms.

Table 7 – LED Flash Pattern for Errors

FIPS Test	LED Pattern					
	LED No.	Color	Red	Green	Blue	Blinks
N3 AES-CBC Encrypt/Decrypt	D12	Red	Y	N	N	1
N3 AES-GCM Encrypt	D12	Red	Y	N	N	2
N3 AES-GCM Decrypt	D12	Red	Y	N	N	3
N3 AES-CCM Encrypt	D12	Red	Y	N	N	4
N3 AES-CCM Decrypt	D12	Red	Y	N	N	5
N3 AES-CMAC Sign	D12	Red	Y	N	N	6
N3 AES-CMAC Verify	D12	Red	Y	N	N	7
N3 AES-CMAC KDF	D12	Red	Y	N	N	8
N3 HMAC KDF	D12	Red	Y	N	N	9
N3 TLS KDF	D12	Red	Y	N	N	10
N3 Triple-DES-CBC Encrypt/Decrypt	D12	Red	Y	N	N	11
N3 RSASP1	D12	Red	Y	N	N	12
N3 ECC CDH	D12	Green	N	Y	N	2
N3 ECDSA Sig Verify	D12	Green	N	Y	N	3
N3 DRBG SHA	D12	Green	N	Y	N	4
N3 RSA Enc and Dec	D12	Green	N	Y	N	5
OpenSSL AESCBC Encrypt/Decrypt	D12	Blue	N	N	Y	1
OpenSSL DSA Sign/Verify	D12	Blue	N	N	Y	2

FIPS Test	LED Pattern					
	LED No.	Color	Red	Green	Blue	Blinks
OpenSSL DRBG CTR	D12	Blue	N	N	Y	3
OpenSSL ECDSA PKV	D12	Blue	N	N	Y	4
OpenSSL ECDSA Sign/Verify	D12	Blue	N	N	Y	5
OpenSSL RSA Sign/Verify	D12	Blue	N	N	Y	6
OpenSSL RSA Encrypt/Decrypt	D12	Blue	N	N	Y	7
OpenSSL HMAC KDF	D12	Blue	N	N	Y	8
OpenSSL X963 KDF	D12	Blue	N	N	Y	9
AES KeyWrap	D12	Blue	N	N	Y	10
AES KeyUnwrap	D12	Blue	N	N	Y	11
TDES KeyWrap	D12	Blue	N	N	Y	12
SP 800-56A KAS	D12	Blue	N	N	Y	13
ECDSA pair wise consistency test	D12	Blue	N	N	Y	4
RSA pair wise consistency test	D12	Blue	N	N	Y	5
DSA pair wise consistency test	D12	Green	N	Y	N	1
Firmware Power-on Tests						
Nitrox device file creation	D14	Red	Y	N	N	1
Nitrox driver load fails	D14	Red	Y	N	N	2
Nitrox micro code load fails	D14	Red	Y	N	N	3
Nitrox pot test failures	D14	Red	Y	N	N	4
Database creation fails	D14	Red	Y	N	N	5
Mgmt daemon has not started successfully	D14	Red	Y	N	N	6
HW RNG for firmware	D12	Blue	N	N	Y	3
Other Firmware States						
HSM Boot stage 1	D10	Red	Y	N	N	No blink
FW integrity Failure state	D10/D12/D14	Red	R	N	N	30 sec on and reboot
HSM Boot stage 2	D10	Red	Y	N	N	Blink (definite)
HSM Boot stage 3(SE-APP initialized Linux handshake not done)	D10	Violet	Y	N	Y	No blink
HSM Linux handshake done, host driver handshake not done	D10	Violet	Y	N	Y	Infinite
HSM PF driver handshake complete	D10	Green	N	Y	N	No blink
HSM admin driver handshake done	D10	Blue	N	N	Y	No blink

5.4 TLS 1.0/1.1/1.2 Cipher Suites

The module supports the algorithms for following cipher suites using FIPS Approved and allowed algorithms and key sizes:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_SHA256
- TLS_RSA_WITH_AES_256_SHA
- TLS_RSA_WITH_DES_CBC3_SHA
- TLS_RSA_WITH_AES_128_SHA256
- TLS_RSA_WITH_AES_128_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

For cipher suites using GCM, the IV is generated per RFC 5288. The module supports GCM cipher suites compatible with SP 800-52.

6 Ports and Interfaces

The module ports and interfaces are described in the below table.

Table 8 – Cavium HSM Ports and Interfaces

Physical Ports/Interfaces	Pins Used	FIPS 140-2 Designation	Name and Description
USB Interface (J2)	USB Interface USB0_DP, USB0_DM	Power No functionality in FIPS mode	USB Interface Not used in FIPS mode
Serial Interface (J3)	3 Pin serial interface - GND, Tx, Rx	N/A No functionality in FIPS mode	Disabled at the hardware level during the firmware load process.
PCIe Interface (P1)	PCIE x8 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) Lane 4 Transmit Side B (33, 34) Receive Side A (35, 36) Lane 5 Transmit Side B (37, 38) Receive Side A (39, 40) Lane 6 Transmit Side B (41, 42) Receive Side A (43, 44) Lane 7 Transmit Side B (45, 46) Receive Side A (47, 48)	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 (7 LEDs, 13 pins)	Status output	Visual status indicator
Tamper PIN	Tamper pin GPIO	Control Input	Tamper pin is used to zeroize the card by zeroizing the master key stored in EEPROM
Power Connector	6 PIN power connector	Power In	External power connector.

7 Identification and Authentication Policy

7.1 Assumption of Roles, Master Partition

The module supports the following roles. One identity is allowed for each role, per partition.

7.1.1 Manufacturer (MFG)

During the manufacturing stage, each HSM goes through the following process:

- An RSA key pair called the HSM FIPS Master Authentication Key (FMAK) is generated on HSM. CSR is requested out of HSM and signed by the Manufacturer Authentication Root Certificate (MARC). The generated certificate is called the HSM FIPS Master Authentication Certificate (FMAC).
- A 256-bit MKBK encrypted with the FMAK public key is loaded into the HSM.
- Program Performance settings and capabilities Appliance Compatibility mode, run random operations, Encrypted channels
- Program Serial Number and Max Operating Temperature

The same above steps are followed by the manufacturer once the HSM is moved to manufacturer reset after manufacturer zeroize.

7.1.2 Master Crypto Officer (MCO)

The master partition supports only the Master Crypto Officer role (MCO). This role is used to configure non-master partitions (create, provision, resize, delete) but cannot access their resources (e.g., cannot manage or use non-master partition keys).

This role is authenticated with username and password (one-factor) and optionally with signature as well (two-factor). Refer to Section 7.3 for details.

7.2 Assumption of Roles, Non-Master Partition Roles

Each Non-Master Partition supports four (4) distinct operator roles as described below. The module enforces the separation of roles using identity-based authentication. Re-authentication is required to change roles.

Except for Pre-CO, concurrent operators are allowed; however, only one operator is allowed per login session.

7.2.1 Pre-Crypto Officer (Pre-CO)

During partition initialization, default credentials are used to create a Pre-CO or a PCO. The Pre-CO is a restricted role primarily for configuring certificates and setting up a PCO. Once a PCO is set up for a partition, the Pre-CO role is no longer accessible.

Because the Pre-CO is essentially a restricted PCO, it does not have its own column in Table 11. Instead, PCO capabilities in Table 11 are marked with an asterisk (*) to indicate Pre-CO can run these services.

This role is authenticated with username and password (one-factor) only.

7.2.2 Partition Crypto Officer (PCO)

This role has access to administrative services of the partition and can configure PCU and AU identities.

This role is authenticated with username and password (one-factor) and optionally with signature as well (two-factor).

7.2.3 Partition Crypto User (PCU)

This role has access to all cryptographic services offered by the partition; its purpose is operational use of the module.

This role is authenticated with username and password (one-factor) and optionally with signature as well (two-factor).

7.2.4 Appliance User (AU)

This role has access to partition audit logs and can create end-to-end encrypted channels. It is to set up and synchronize clusters.

This role is authenticated with username and password (one-factor) only.

7.3 Authentication

The module enforces identity-based authentication. A role is explicitly selected at authentication; the MCO role is associated with the Master Partition and the PCO and PCU roles are associated with user partitions (see Section 7.1 for details). The module allows one identity per role, per partition.

Table 9 – Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
MFG	This role sets the identity, serial number, performance settings and max operating temperature	Manufacturer License certificate-based authentication	RSA signature
MCO	This role has access to administrative services offered by the module or HSM	Identity-based operator authentication	Username and password; optional RSA signature (2FA)
Pre-CO	This role is an optional role with limited functionality, eventually transition into PCO	Identity-based operator authentication	Username and password
PCO	This role has access to administrative services of the partition	Identity-based operator authentication	Username and password; optional RSA signature (2FA)
PCU	This role has access to all crypto services offered by the partition	Identity-based operator authentication	Username and password; optional RSA signature (2FA)
AU	This role has access to partition audit logs and Appliance secure channel key	Identity-based operator authentication	Username and password

Table 10 – Strength of Authentication Mechanism

Authentication Mechanism	Strength of Mechanism
Username and password	The password is a minimum of 7 characters, case-sensitive alpha-numeric. As such there are (26*2+10)^7 = 62^7 possible minimum-length passwords, and the false acceptance rate is 1 in 62^7 which is less than 1 in 1,000,000. A maximum of 20 password attempts are possible before permanent lockout. Therefore, the probability of false authentication over any timeframe is 20 in 62^7, which is less than 1 in 100,000. (The number of allowed login attempts prior to lockout is configured during module initialization but cannot exceed 20.) Lockout of MCO automatically zeroizes the module. In all other cases, lockout can be unset by destroying the partition.
RSA Signature	Authentication is performed using SHA-256 based RSA 2048-bit PKCS#1-v1.5 signatures (provides 112 bits of strength). Corresponding public key is associated with the identity (for Manufacturing role, it is part of FW image). The probability that a random attempt will succeed, or a false acceptance will occur, is approximately 1 in 2^112, which is less than 1 in 1,000,000. For each failed signature verification, the module will block for 2 seconds. Based on this maximum rate, the probability that a random attempt will succeed in a one minute period is approximately 30 in 2^112, which is less than 1 in 100,000.

7.4 Roles, Services, and CSP Access

G = Generate: The module generates the CSP.

O = Output: The module reads the CSP out of the module.

I = Input: 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.

E = Execute: The module executes or uses the CSP.

Table 11– Roles, Services and CSPs

MCO	PCO	PCU	MFG	AU	Un-auth	Service	Description	Commands	Cryptographic Keys/CSPs
X			X		X	MP Zeroize	Zeroize the master partition. Can be configured to be allowed by CO only.	CN_ZEROIZE	Z: All keys in Set 1 of Table 12
X						MP Factory Reset	Factory-reset the master partition	CN_ZEROIZE	Z: All keys in Sets 1,2 of Table 12
X						MP Vendor Zeroize	Zeroize all data	CN_VENDOR_ZEROIZE	Z: All keys in Set 1,2,3 of Table 12
	X	X		X	X	Partition Zeroize	Zeroize a given partition. Can be configured to be allowed by CO only	CN_ZEROIZE	Z: All keys in Set 4 of Table 12

MCO	PCO	PCU	MFG	AU	Un-auth	Service	Description	Commands	Cryptographic Keys/CSPs
	X					Partition Factory Reset	Factory-reset a given partition	CN_ZEROIZE	Z: All keys in Set 4,5 of Table 12
X						Partition Delete	Delete a partition & all associated keys	CN_DELETE_PARTITION	Z: All keys in Set 4,5,6 of Table 12
X	X	X	X	X	X	Session Management	Management services for open, status of sessions.	CN_APP_INITIALIZE CN_APP_FINALIZE CN_OPEN_SESSION CN_CLOSE_SESSION CN_GET_SESSION_ INFO	Z: Session Keys Stored in RAM
X	X	X	X	X	X	Session Management – Close	Management services for closing all sessions.	CN_CLOSE_ALL_ SESSIONS	Z: Session Keys Stored in RAM
X	X					Partition Application Session Close (All)	Close sessions of all Applications tied to a Partition.	CN_CLOSE_ PARTITION_ SESSIONS	Z: Session Keys Stored in RAM
X	X	X	X	X	X	Basic HSM Info	Obtain basic information of the HSM.	CN_TOKEN_INFO CN_PARTITION_INFO CN_GET_HSM_LABEL CN_ALL_PARTITION_ INFO CN_GET_POLICY_SET CN_GET_M_VALUE	
X	X	X	X	X	X	Read Firmware Version String	Obtain firmware version.	CN_GET_VERSION	
X	X	X	X	X	X	Read or delete coredump file	Read-out or delete coredump if it exists	CN_GET_CORE_DUMP CN_DELETE_CORE_DUMP	
					X	Enables encrypted communication channel	Create E2E session.	CN_ENCRYPT_SESSION CN_AUTHORIZE_SESSION	G: E2E TLS Session Symmetric Key Set, E2E TLS Session HMAC Key Set E: PAC
X	X	X	X	X	X	Login to a Session	Allows login to a session. Public key is used to verify user signatures, optionally in 2-factor authentication.	CN_LOGIN	E: PEK, Two-Factor Authentication Public Key (In case of 2FA only) I: Password
X	X	X		X		Logout of a Session	Allows logout of a session.	CN_LOGOUT	
X	X *	X		X		Change User Password	Requires user to be logged in. Updates Passwords and Public key for 2-factor authentication.	CN_CHANGE_PSWD	E: PEK I: new password, new public key Z: Old password
X			X			Manufacturer Settings	Manufacturer Controlled Settings run by manufacturer for the first time and MCO can do it later.	CN_MASTER_CONFIG CN_CERT_AUTH_ GET_CERT_REQ CN_CERT_AUTH_ STORE_CERT CN_STORE_VENDOR_PRE_SHARED_ KEY (CN_STORE_KBK_SHARE) CN_SET_KBK_PRIMARY	G: FMAK, MFDEK E: Manufacturer License Validation Key I: MARC, FMAC, MFKBK

MCO	PCO	PCU	MFG	AU	Un-auth	Service	Description	Commands	Cryptographic Keys/CSPs
X						Initialize HSM	Commands and services to initialize the module.	CN_INIT_TOKEN CN_GEN_PSWD_ENC_KEY CN_CREATE_CO CN_INIT_DONE CN_CERT_AUTH_STORE_CERT CN_CERT_AUTH_GET_CERT_REQ CN_CERT_AUTH_STORE_CERT CN_STORE_USER_PRE_SHARED_KEY (CN_STORE_KBK_SHARE) CN_SET_KBK_PRIMARY	G: PEK, MMEK E: PEK, MFDEK O: CSR for FMAKI: Host PswdEncKeyPublic Key, AOAC, Password, Two-Factor Authentication Public key, AOTAC
				X		Secure Boot	Commands to identify the hosts are of Cavium.	CN_CERT_AUTH_GET_CERT CN_CERT_AUTH_RECV_PEER_CERT CN_CERT_AUTH_SECURE_BOOT	E: MARC to validate HOST_ID cert, HOST_ID cert to validate signature on challenge SecureBootAuth Public Key, FMAC
X						Firmware Update	Updates adapter with Cavium signed firmware images. Adapter has to be rebooted to use the new firmware.	CN_FW_UPDATE_BEGIN CN_FW_UPDATE CN_FW_UPDATE_END	E: Manufacturer Firmware Validation Key I: Manufacturer Firmware Validation Key, Manufacturer License Validation Key Z: Optionally Zeroize the HSM keys.
X						Other MCO Operations	Misc. MCO Operations.	CN_SLAVE_CONFIG CN_INVOKE_FIPS CN_GET_RSA_CACHE_SIZE CN_GET_HSM_DIAG_INFO CN_PARTN_STORAGE_GET CN_PARTN_STORAGE_UPDATE CN_PARTN_STORAGE_DELETE	
X						Partition Management	Commands and services to manage partitions.	CN_CREATE_PARTITION CN_DELETE_PARTITION CN_RESIZE_PARTITION CN_GET_PARTITION_COUNT CN_ALL_PARTITION_INFO	G: PAK key pair, PMEK E: FMAK, MFDEK W: PAC Z: All partition keys

MCO	PCO	PCU	MFG	AU	Un-auth	Service	Description	Commands	Cryptographic Keys/CSPs
X						MCO Backup and Restore	Allows MCO to take back up using KBK derived from pre-loaded MKBK, OKBK. MCO uses find key in to get the key handles in a partition.	CN_BACKUP_BEGIN CN_BACKUP_CONFIG CN_BACKUP_USERS CN_BACKUP_KEY CN_BACKUP_END CN_RESTORE_BEGIN CN_RESTORE_CONFIG CN_RESTORE_USERS CN_RESTORE_KEY CN_RESTORE_END CN_BACKUP_OBJECT	G: KBK, Backup session key E: MFKBK, OKBK, Optionally POKBK, KBK O: POTAC, All keys NIST AES wrapped with KBK I: User passwords and Two-Factor Authentication Public Keys, All keys NIST AES wrapped with KBK, new POTAC verify the owner ship Z: Backup session key
	X					PCO Backup and Restore	PCO uses find key in to get the key handles in a partition.	CN_BACKUP_BEGIN CN_CREATE_OBJECT CN_WRAP_KBK (Modes: KBK_WRAP_WITH_KEK, KBK_WRAP_WITH_CERT_AUTH_DERIVED_KEY, KBK_WRAP_WITH_RSA, KBK_USING_PRE_SHARED_KEYS) CN_BACKUP_CONFIG CN_BACKUP_USERS CN_BACKUP_KEY CN_BACKUP_END CN_RESTORE_BEGIN CN_GENERATE_KEY_PAIR CN_UNWRAP_KBK (Modes: KBK_WRAP_WITH_KEK, KBK_WRAP_WITH_CERT_AUTH_DERIVED_KEY, KBK_WRAP_WITH_RSA) CN_RESTORE_CONFIG CN_RESTORE_USERS CN_RESTORE_KEY CN_RESTORE_OBJECT CN_RESTORE_END	G: KBK Wrapping RSA key pair, POKBK, KBK E: KLK or KBK Wrap RSA public key or SAZ, MFKBK, OKBK, POKBK, KBK, POKBK, O: wrapped Partition KBK, User passwords and Two-Factor Authentication Public Keys, All user keys, I: KBK wrap public key, All keys NIST AES wrapped with KBK, User passwords and Two-Factor Authentication Public Keys, All user keys, Z: SAZ
X						MCO Partition Data Management	Commands to manage Unclassified data storage mainly used to maintain network IP addresses.	CN_PARTN_STORAGE_UPDATE CN_PARTN_STORAGE_GET CN_PARTN_STORAGE_DELETE	

MCO	PCO	PCU	MFG	AU	Un-auth	Service	Description	Commands	Cryptographic Keys/CSPs
	X *					Partition Initialization	Commands to initialize the partition and claim ownership of the partition, reset resources.	CN_INIT_TOKEN CN_GEN_PSWD_ ENC_KEY CN_CREATE_CO CN_INIT_DONE CN_CERT_AUTH_ GET_CERT_REQ CN_CERT_AUTH_ STORE_CERT CN_STORE_USER_ PRE_SHARED_ KEY CN_ACC_DEV_RESET (CN_STORE_KBK_SHARE) CN_SET_M_VALUE CN_SET_NODEID CN_SET_KBK_PRIMARY	G: PEK, Partition's Masking Key E: PEK, FMAK O: CSR for PAK I: Host PswdEncKeyPublicKey, Password, Two-Factor Authentication Public key, POAC, POTAC, POKBK
	X					PCO UserManagement	Commands to manage users in the partition.	CN_CREATE_USER CN_DELETE_USER CN_LIST_USERS CN_GET_LOGIN_ FAILURE_CNT CN_CREATE_PRE_OFFICER CN_CREATE_APPLIANCE_U SER	E: PEK to decrypt and store, PMEK to encrypt the password and store it in database I: password and new Public key Z: all session keys
X	X					SecureAuth based on Certificates	Commands used for mutual authentication and key agreement between two partitions/entities of same Partition owner on Cavium HSM.	CN_CERT_AUTH_ GET_CERT CN_CERT_AUTH_ GET_SOURCE_ RANDOM CN_CERT_AUTH_ VALIDATE_PEER_ CERTS CN_CERT_AUTH_ GET_CERT CN_CERT_AUTH_ VALIDATE_PEER_ CERTS CN_CERT_AUTH_ SOURCE_KEY_ EXCHANGE	G: SAZ E: POTAC to verify peer POAC, MARC to verify peer PAC and FMAC, peer PAC to verify peer signature, local PAK to sign responder's challenge, local PAK to sign initiator's challenge O: FMAC, PAC, POAC, I: Peers FMAC, PAC, POAC,

MCO	PCO	PCU	MFG	AU	Un-auth	Service	Description	Commands	Cryptographic Keys/CSPs
X	X					Cloning Protocol	Cloning: Clone Masking of a Partition to a different Partition of the same owner.	CN_CLONE_SOURCE_INIT CN_CLONE_SOURCE_STAGE1 CN_CLONE_TARGET_INIT CN_CLONE_TARGET_STAGE1	G: KAS key pair, CSSZ and KAS, Partition's Cloning Private Key, KAS keying material (Partition's Cloning Session Key, Partition's Cloning Session MAC Key) E: KAS keying material for masking key encryption and mac tag generation and peer mac tag verification, KAS keying material for presumed data encryption and mac tag generation, KAS keying material to decrypt the masking key, validate MAC tag. Partition Cloning Initiator Public Key, Partition Cloning Responder Public Key, Partition's Masking Key, SAZ, Partition Cloning ECC Domain Parameter Set O: Partition Cloning Initiator Public Key, Partition Cloning Responder Public Key, Partition's Masking Key I: Partition Cloning Initiator Public Key, Partition Cloning Responder Public Key, Partition's Masking Key Z: CSSZ, SAZ, and KAS keying material (Partition's Cloning Session Key, Partition's Cloning Session MAC Key)
	X *					Key Transportation	A SP 800-56 A/B protocol to generate a shared KLK on host and Partition.	CN_GEN_KEY_ENC_KEY	G: Partition's KeyLoading private/public RSA/ECC key pair, KLSZ, KLK, I: Host RSA/ECC KeyLoading Public Key Z: KLSZ, Partition KeyLoading private/public key pair

MCO	PCO	PCU	MFG	AU	Un-auth	Service	Description	Commands	Cryptographic Keys/CSPs
	X	X		X		PCU Key Management	Key can be shared with multiple users to use it for crypto operations. Tombstone feature is added to support key deletions in cluster modes. Note: clusters are fully maintained out of HSM and this is just to enable the feature.	CN_EXTRACT_MASKED_OBJECT CN_INSERT_MASKED_OBJECT CN_DESTROY_OBJECT CN_GET_ATTRIBUTE_VALUE CN_GET_ATTRIBUTE_SIZE CN_GET_ALL_ATTRIBUTES_SIZE CN_GET_ALL_ATTRIBUTES_VALUE CN_MODIFY_OBJECT CN_FIND_OBJECTS CN_FIND_OBJECTS_FROM_INDEX CN_GENERATE_KEY CN_GENERATE_KEY_PAIR CN_GENERATE_PBE_KEY CN_EXPORT_PUB_KEY CN_SHARE_OBJECT CN_GET_OBJECT_INFO CN_TOMBSTONE_OBJECT CN_DELETE_TOMBSTONED_OBJECT CN_UNWRAP_KEY CN_WRAP_KEY CN_DERIVE_KEY CN_FIND_OBJECTS_USING_COUNT CN_MODIFY_KEY_OWNER	G: All General Purpose User CSPs, General Purpose User Public Keys E: Partition's Masking Key, KLK or user provided wrapping Key, PEK specified user key, All General Purpose User CSPs, O: General Purpose User CSPs in wrapped form General Purpose User Public Keys I: Imported keys in wrapped form Z: General Purpose User CSPs, General Purpose User Public
X	X	X		X		Find Key handles	Users can find key handles based on search criteria like key type or label. MCO/PCO use it as part of backup service. Hash of key handles in order to check if clusters are in sync.	CN_FIND_OBJECTS CN_FIND_OBJECTS_FROM_INDEX CN_FIND_OBJECTS_USING_COUNT CN_FIND_ALL_OBJECTS_USING_COUNT CN_ADMIN_GET_PARTN_KEYHANDLES_HASH	
				X		PCU Key Management – Special	Unwrap only RSA Key	CN_UNWRAP_KEY CN_FIND_OBJECT CN_DELETE_OBJECT	E: KLK O: Asymmetric Public Key (RSA only) I: Asymmetric Private Key (RSA only) Z: Asymmetric Private Key (RSA only)

MCO	PCO	PCU	MFG	AU	Un-auth	Service	Description	Commands	Cryptographic Keys/CSPs
		X		X		PCU Crypto Offload	CN_ME_PKCS and CN_ME_PKCS_LARGE are RSA 2K and 3K operations. Appliance user is allowed to use the imported RSA key.	CN_SIGN CN_VERIFY CN_ECC_DH CN_NIST_AES_WRAP CN_ALLOC_SSL_CTX CN_FREE_SSL_CTX CN_GEN_PMK CN_FIPS_RAND CN_ME_PKCS_LARGE CN_ME_PKCS CN_FECC CN_HASH CN_HMAC CN_ENCRYPT_DECRYPT	E: specified user key
	X			X		Audit Logs – PCO / Appliance		CN_PARTN_GET_ AUDIT_DETAILS CN_PARTN_GET_ AUDIT_LOGS CN_PARTN_GET_ AUDIT_SIGN CN_PARTN_ACK_ AUDIT_SIGN CN_PARTN_ACK_AUDIT_SIGN CN_PARTN_GET_AUDIT_LOGS CN_PARTN_GET_AUDIT_DETAILS	E: PAK, FMAK
X						Audit Logs – MCO		CN_FINALIZE_LOGS	
X	X					HSM policies – MCO Partition policies – PCO	MCO: Enable audit logs for partition (Sticky policy) PCO: Enable/Disable of crypto/mgmt. logs	CN_SET_POLICY	
		X				SSL Protocol Packet Processing	These API can understand the SSL/TLS protocol semantics and optimized to do multiple sequential crypto operations on the given input data. For example: Encrypt/decrypt record will do HMAC comparison in addition to the symmetric crypto operation.	MAJOR_OP_RSASERVER_LARGE MAJOR_OP_RSASERVER MAJOR_OP_HANDSHAKE MAJOR_OP_OTHER MAJOR_OP_FINISHED MAJOR_OP_RESUME MAJOR_OP_ENCRYPT_DECRYPT_RECORD MAJOR_OP_ECDH	E: TLS Session Symmetric Key Set and TLS Session HMAC key part of SSL Context
	X	X				MofN authentication	To execute a service or use key ‘m’ users of ‘n’ allowed users should approve.	CN_GET_TOKEN CN_APPROVE_TOKEN CN_LIST_TOKENS CN_TOKEN_TIMEOUT CN_DELETE_TOKEN	
X						Load KBK	Load Manufacturer / AO / PO KBK	CN_LOAD_KBK	I: MFKBK, OKBK, POKBK

PCO capabilities in Table 11 are marked with an asterisk (*) to indicate Pre-CO can run these services.

8 Keys and Certificates

8.1 Definition of Critical Security Parameters (CSPs)

The Manufacturer FIPS Data Encryption Key (MFDEK) and HSM Master Partition Master Encryption Key are stored in plaintext form in the EEPROM. The Partition Master Encryption Key (PMEK) is stored encrypted under the HSM Master Partition Master Encryption Key. All other keys and CSPs stored in the persistent memory are encrypted by the MFDEK, HSM Master Partition Master Encryption Key, or PMEK. All general-purpose user CSPs are generated/created by the PCU and these CSPs can be shared between multiple PCUs.

Note: All the DRBGs are supplied with 6 blocks of size of 48-bytes. This will provide an unmodified, combined nonce and seed of 256 bits of security.

D: Manually Deleted

E: Erased right after used

S: Deleted on session close.

Column “Set” categorize CSPs as set 1 to 6 and links with Table-11 to identify the CSPs zeroized in each service.

Table 12 – Private Keys and CSPs

Name	Description and Usage	Set
HSM CSPs		
DRBG Entropy	The entropy material for the FIPS Approved DRBG. Each version of the DRBG has its own DRBG Entropy CSP.	1, E
CTR_DRBG Internal State #C821	The internal state for the FIPS Approved DRBG.	1, E
CTR_DRBG Internal State #680	The internal state for the FIPS Approved DRBG.	1, E
HASH_DRBG Internal State	The internal state for the FIPS Approved SHA DRBG.	1, E
Manufacturer FIPS Data Encryption Key (MFDEK)	AES 256-bit key used to encrypt manufacturer keys stored in persistent storage of the HSM.	3
HSM Master Partition Master Encryption Key (MMEK)	AES 256-bit key used to encrypt Master Partition CSPs and authentication data stored in persistent storage of the HSM.	1
Partition Master Encryption Key (PMEK)	AES 256-bit key used to encrypt partition CSPs and authentication data stored in persistent storage of the HSM.	1
HSM FIPS Master Authentication Key (FMAK)	A unique 2048-bit RSA private key. Used to identify the HSM when in the FIPS operating mode.	3
Partition Authentication Key (PAK)	A unique 2048-bit RSA private key used to identify the HSM Partition.	1, 6
SecureAuth Shared Secret (SAZ)	Shared secret Z for SP 800-56B KAS2, using PAK and POAC	1, 4, E, S
Authentication CSPs		
PswdEncKeyRSAPrivate Key	2048-bit RSA Private Key, used in SP 800-56B KAS to generate PswdEncKey.	1, 4, E
PswdEncKey (PEK)	AES-256 key, for encrypting User passwords during user creation and authentication.	1, 4
Login Passwords	String of 7 to 32 alphanumeric characters.	1, 4

Name	Description and Usage	Set
Key Loading CSPs		
Partition's KeyLoading Private Key	ECC 521-bit or RSA 2048-bit key used in SP 800-56A C (2,0, ECC DH) or SP 800-56B KAS2 to agree on Z during key loading.	1, 4, E
Partition's KeyLoading Shared Secret (KLSZ)	Shared secret Z for SP 800-56A C (2,0, ECC DH) or SP 800-56B KAS2.	1, 4, E
Partition's Key Loading Key (KLK)	A 256-bit AES key derived from Z, used to decrypt the imported CSPs.	1, 4
Backup and Restore Keys		
Manufacturer FIPS Key Backup Key (MFKBK)	AES 256-bit key used to derive KBK.	3
HSM Owner KBK (OKBK)	AES 256-bit key used to derive KBK.	2
Partition Owner KBK (POKBK)	AES 256-bit key used to derive KBK.	1, 5
HSM Key Backup Key (KBK)	Key used to encrypt/decrypt the Backup Session Key.	1, 4
Backup Session Key	Key used to backup and restore partition data.	1, 4, E
Cloning Keys		
Partition's Cloning Private Key	ECC 521-bit or RSA 2048-bit ephemeral Private Key used in SP 800-56A C (2,0, ECC DH) or SP 800 -56B KAS2 -bilateral -confirmation key agreement to generate shared secret Z. At HSM Partition level, used to establish secure channel for cloning process (to export Partition's Masking Key).	1, 4, E
Partition's Cloning Shared Secret (CSSZ)	Shared secret Z for SP 800-56A C (2,0, ECC DH) or SP 800-56B KAS2 -bilateral -confirmation scheme.	1, 4, E
Partition's Cloning Session Key	AES 256 key for encryption and decryption of Partition's Masking Key.	1, 4, E
Partition's Cloning Session MAC Key	HMAC SHA256 key used for key confirmation during SP 800-56A key agreement.	1, 4, E
Partition's Masking Key	AES-256 key, for key wrapping. Used to import/export CSPs and masked objects.	1, 4
General Purpose User CSPs		
Asymmetric Private Keys	RSA/DSA/ECDSA/ECDH general purpose keys.	1, 4, D
Asymmetric Private Session Keys	RSA/DSA/ECDSA/ECDH general purpose session keys.	1, 4, D, S
Symmetric Keys	Triple-DES or AES general purpose keys.	1, 4, D
Symmetric Session Keys	Triple-DES or AES general purpose session keys.	1, 4, D, S
HMAC Keys	HMAC general purpose keys (minimum key size of 160 bits).	1, 4, D
HMAC Session Keys	HMAC session general purpose keys (minimum key size of 160 bits).	1, 4, D, S
TLS Session ECDH Key	Used for key agreement as part of TLS-1.0/1.1/1.2 handshake protocol.	1, 4, D
TLS Session Symmetric Key Set	AES 128, 192, 256 or Triple-DES keys used for encrypting TLS sessions.	1, 4, D, S
TLS Session HMAC key	HMAC key used in SSL session (minimum key size of 160 bits).	1, 4, D, S
E2E Session Keys		
E2E TLS Session Symmetric Key Set	AES 128 Key used for encrypting/decrypting E2E session data.	1, 4, D, S
E2E TLS Session HMAC keys	HMAC keys used in E2E session.	1, 4, D, S

8.2 Definition of Public Keys

The module contains the following public keys:

Table 13 – Public Keys

Name	Description and Usage	Sets
HSM Keys		
Manufacturer Firmware Integrity Check Keys	RSA 2048-bit public keys used to check the integrity of the SW images booted. The SW image is signed by the manufacturer using a RSA private key.	
Manufacturer Firmware Update Validation Key	RSA 2048-bit public key used to authenticate new SW images uploaded into the module. The SW image is signed by the manufacturer using an RSA private key and the signature is verified before upgrading to the new image using the public key.	
Manufacturer Debug Firmware Update Validation Key	RSA 2048-bit public key used to authenticate debug enabled new SW images loaded into the module. The SW image is signed by the manufacturer using a RSA private key and the signature is verified before upgrading to the new image using this public key. On successful upgrade HSM is zeroized before booting into debug image.	
Manufacturer License Validation Key	RSA 2048-bit public key used to authenticate the manufacturer role.	3
Manufacturer Authentication Root Cert. (MARC)	RSA 2048-bit public key certificate, used to issue FMAC certificates.	3
HSM FIPS Master Authentication Certificate (FMAC)	RSA 2048-bit public key certificate of FMAK. Used to identify the HSM FIPS operating mode.	3
SecureBootAuth Public Key	RSA 2048-bit public key used to verify authenticity of the host system.	2
Administrative Keys		
HSM/Adapter Owner Trust Anchor Certificate (AOTAC)	RSA 2048-bit public key certificate used as trust anchor of MCO.	2
HSM/Adapter Owner Authentication Certificate (AOAC)	RSA 2048-bit public key certificate of FMAK. Used to identify the HSM owner.	2
Partition Authentication Certificate (PAC)	RSA 2048-bit public key certificate of PAK. Used to identify the Partition.	1, 6
Partition Owner Trust Anchor Certificate (POTAC)	RSA 2048-bit public key certificate used as trust anchor of PCO.	1, 5
Partition Owner Authentication Certificate (POAC)	RSA 2048-bit public key certificate of PAK. Used to identify the Partition owner.	1, 5

Name	Description and Usage	Sets
Key Backup/Cloning Keys		
Partition Cloning Initiator Public Key	ECC 521-bit ephemeral public key used in SP 800-56A C (2,0, ECC DH) key agreement or RSA 2048-bit ephemeral public key used in SP 800-56B KAS2 - bilateral -confirmation key agreement to generate shared secret Z.	1, 4, E
Partition Cloning Responder Public Key	ECC 521-bit ephemeral public key used in SP 800-56A C (2, 0, ECC DH) key agreement or RSA 2048-bit ephemeral public key used in SP 800-56B KAS2 - bilateral -confirmation key agreement to generate shared secret Z.	1, 4, E
Partition Cloning ECC Domain Parameter Set	Set EE per SP 800-56A Table 2.	1, 4, E
Authentication Keys		
Partition PswdEncKeyPublicKey	RSA 2048-bit public key generated by the partition to be used in SP 800-56B key agreement to generate PswdEncKey.	1, 4, E
Host PswdEncKeyPublicKey	RSA 2048-bit public key loaded by the host to be used SP 800-56B key agreement to generate PswdEncKey.	1, 4, E
Two-Factor Authentication Public Key or MofN Authentication Key	RSA 2048-bit public key used to verify signature on encrypted passwords during user creation and login and/or to verify signatures on MofN authentication tokens.	1, 4
General Purpose Keys		
User Public Keys	RSA/DSA/ECDSA/ECDH public keys.	1, 4
User Public Session Keys	RSA/DSA/ECDSA/ECDH public session keys.	1, 4

8.3 Definition of Session Keys

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. PCU can share the session keys with other users, so that other sessions can use it.
- Every session in an application will have access to the keys created by every other session in the same application.
- When a session is closed, the session keys created by that session get destroyed. If the key is shared, then it will be deleted only after closing all the sessions sharing this key.

9 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.

10 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. Power-Up Self Tests (KAT)
      a. Firmware Integrity Tests (RSA 2048-bit SHA-256 signature verification and a 32-bit CRC).
      b. Nitrox Library
         - AES 128-bit CBC Encrypt & Decrypt (#C839)
         - AES 128-bit GCM Encrypt & Decrypt (#C839)
         - AES 128-bit CCM Encrypt & Decrypt (#C839)
         - AES 128-bit CMAC Sign and Verify (#C839)
         - SP 800-108 128-bit CMAC KDF in Counter (#C839)
         - SP 800-108 HMAC SHA256 KDF in Counter (#C839)
         - TLS KDF (#C840)
         - Triple-DES CBC Encrypt & Decrypt (Triple DES #1131)
         - RSASP 2048-bit (#C839)
         - ECC CDH P256 and P384 (#C829)
         - ECDSA P256 Verify using SHA-1, SHA256, SHA384, SHA512 (#C829, and SHS #1780)
         - SP 800-90A SHA512 HASH_DRBG (#C830)
         - RSA 2048-bit Encrypt and Decrypt (#C839 and #A1955)

      c. OpenSSL Library
         - AES 128-bit CBC Encrypt & Decrypt (#C819)
         - SP 800-90A CTR_DRBG (#C821)
         - SP 800-90A CTR_DRBG (DRBG #680)
         - DSA 2048-bit SHA-256 Sig Gen and Sig Ver (#C823)
         - ECDSA PKV, Sig Gen and Sig Ver using P256 with SHA-1, SHA256, SHA384, SHA512 (#C825 and SHS #C820)
         - RSA 2048-bit Sig Gen, Sig Ver (#C824, #A1953 and #A1954)
         - RSA 2048-bit Encrypt and Decrypt (#A1953 and #A1954)
         - SP 800-108 HMAC SHA256 KDF (#C826 and #C822)

      d. Others
         - SP 800-56A KAS using P521 and HMAC SHA512 (#A1952)
         - SP 800-38F AES Key Wrap and Unwrap (Cert. #1263, LiquidSecurity Keywrap)
         - SP 800-38F Triple-DES Key Wrap and Unwrap (Cert. #1263, LiquidSecurity Keywrap, and TDES CBC #C1169)

B. Conditional Self-Tests
- ECDSA Pairwise Consistency Test (#C829 and #C825)
- RSA Pairwise Consistency Test (#C824, #A1954, and #A1955)
- DSA Pairwise Consistency Test (#C823)
- DRBG, SP800-90A health tests (#680, #C821, and #C830)
- HW RNG Continuous Number Test
- Firmware load test (RSA Signature Verification) – RSA 2048-SHA512

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. EEPROM Test
    c. NOR Flash Test
    d. 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. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
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.
16. The module shall be configured for FIPS operation by following the first-time initialization procedure described in User Manual and C-API Specification (CNN35XX-NFBE-SDK-UserGuide).

11 Physical Security Policy

11.1 Physical Security Mechanisms

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: The module's hardness testing was only performed at ambient temperature (23°C); no assurance is provided for Level 3 hardness conformance at any other temperature.

11.2 Tamper Evidence

The module is coated in hard epoxy, such that any physical breach attempt leaves behind evidence of tamper. This is shown in the figure below.

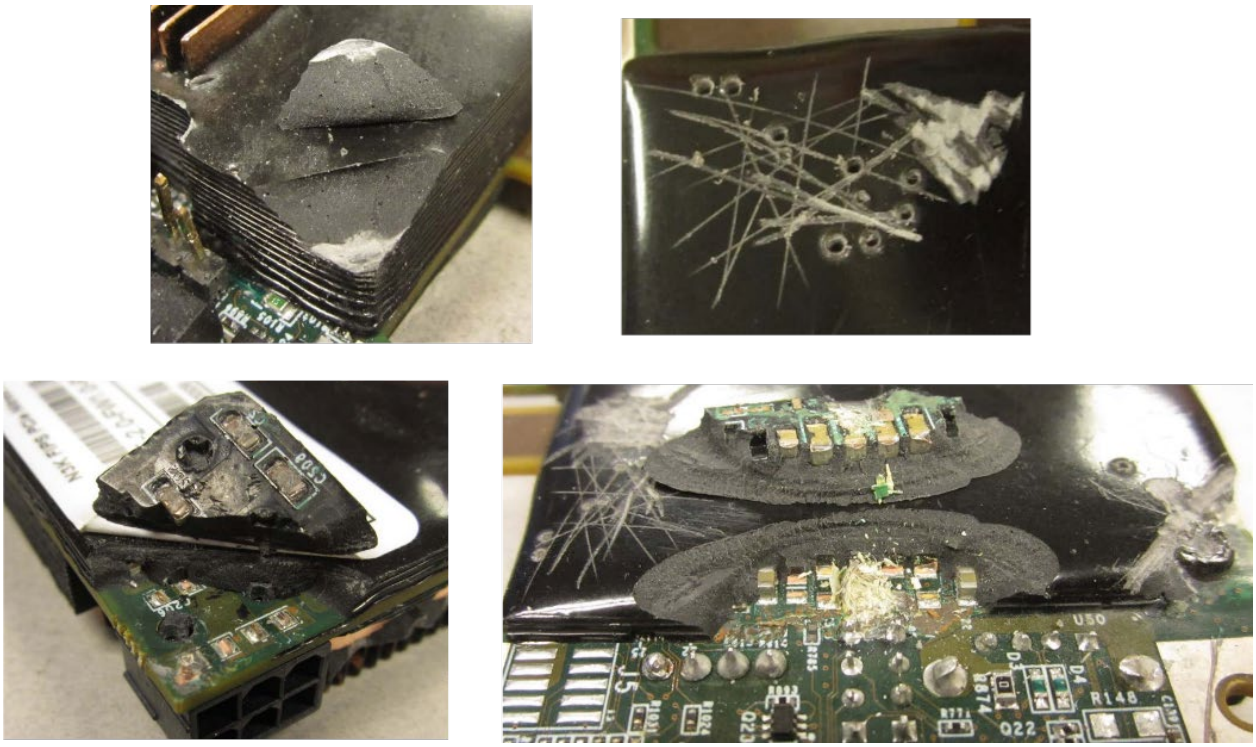

Figure 2 – Cryptographic Module Showing Tamper Evidence

Top: Minor tamper to the epoxy only

Bottom: Major tamper, damaging circuitry

While the module is designed to prevent successful tampering (any physical breach to module circuitry is likely to destroy the module, as per FIPS 140-2 Level 3 Physical Security requirements), the module should still be checked periodically for attempts. Guidelines are provided in the table below.

Table 14 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Epoxy Coating	12 Months	Examine surface of module for scratched or damaged epoxy, especially if circuitry shows.

If the module is found to be meaningfully damaged or tampered with (e.g., circuitry is showing, or other significant damage has occurred), it should be removed from usage and destroyed.

12 Mitigation of Other Attacks Policy

No mitigation of other attacks is implemented by the module.

13 References

1. NIST Key Wrap Specification, SP 800-38F, December 2012.
2. NIST Special Publication 800-38D November 2007.
3. NIST Special Publication 800-56A, March 2007.
4. NIST Special Publication 800-56B, August 2009.
5. NIST Special Publication 800-57 Part-1, May 2006.
6. FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013.
7. FIPS PUB 140-2, FIPS Publication 140-2 Security Requirements for Cryptographic Modules.
8. NIST Special Publication 800-90A, January 2012
9. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program
10. NIST Special Publication 800-131Ar2, March 2019.
11. FIPS PUB 186-2 Digital Signature Standard (DSS), Jan 2000.
12. NIST Special Publication 800-133 Revision 1, July 2019
13. NIST Special Publication 800-108, October 2009
14. NIST Special Publication 800-135 Revision 1, December 2011

14 Definitions and Acronyms

MCO – Master Crypto Officer

PCO – Partition Crypto Officer

PCU – Partition Crypto User

HSM – Hardware Security Module

KBK – Key Backup Key

KLK – Key Loading Key

KAT – Known Answer Test

KAS – Key Agreement Scheme

SR-IOV – Single Root I/O Virtualization

2FA – 2 Factor Authentication