ULTRA

Ultra Intelligence & Communications
FIPS 140-2
Non-Proprietary Security Policy
Level 2 Validation

3e-636 CyberFence Cryptographic Module

HW Version (1.0)
FW Version (5.2)

Security Policy Version 1.4

October 3, 2022

ULTRA

Table of Contents

Glossary of terms

A&A	Authentication and Authorization
AP	Access Point
CO	Cryptographic Officer
IP	Internet Protocol
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
HTTPS	Secure Hyper Text Transport Protocol
LAN	Local Area Network
MAC	Medium Access Control
PSK	Pre-shared Key
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SRDI	Security Relevant Data Item
SSID	Service Set Identifier
TLS	Transport Layer Security
WAN	Wide Area Network
WLAN	Wireless Local Area Network

1. Introduction

This is a non-proprietary Cryptographic Module Security Policy for the 3e-636 CyberFence Cryptographic Module (hereafter referred to as module) with Hardware Version: 1.0 and Firmware Version: 5.2 from Ultra. This Security Policy describes how the module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at https://csrc.nist.gov/Projects/cryptographic-module-validation-program/publications.

1.1 Cryptographic Module Definition

The module primarily acts as a boundary protection device. Using IPSec based VPN or IEEE 802.3 VLAN encryption technology, it sets up a secured channel between LAN and WAN networks. Furthermore, it employs firewall and industrial control protocol packet inspection to provide defense-in-depth capabilities to prevent malicious attacks.

The module is a multiple-chip embedded cryptographic module for the purposes of FIPS 140-2. The cryptographic boundary is defined as a tamper-resistant opaque metal enclosure, protected by tamper evidence tape intended to provide physical security. There is only one operational mode for the device which is FIPS mode. Figure 1 below shows the module with the tamper evidence labels (TELs).

Figure 1 – 3e-636 CyberFence Cryptographic Module

1.2 Cryptographic Module Validation

The module is validated at the FIPS 140-2 Section levels listed in Table 1 below. The overall security level of the module is 2.

Table 1: Module Security Level

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
Overall		2

2. Ports & Interfaces

The module contains a simple set of interfaces, as shown in Figure 2 below:

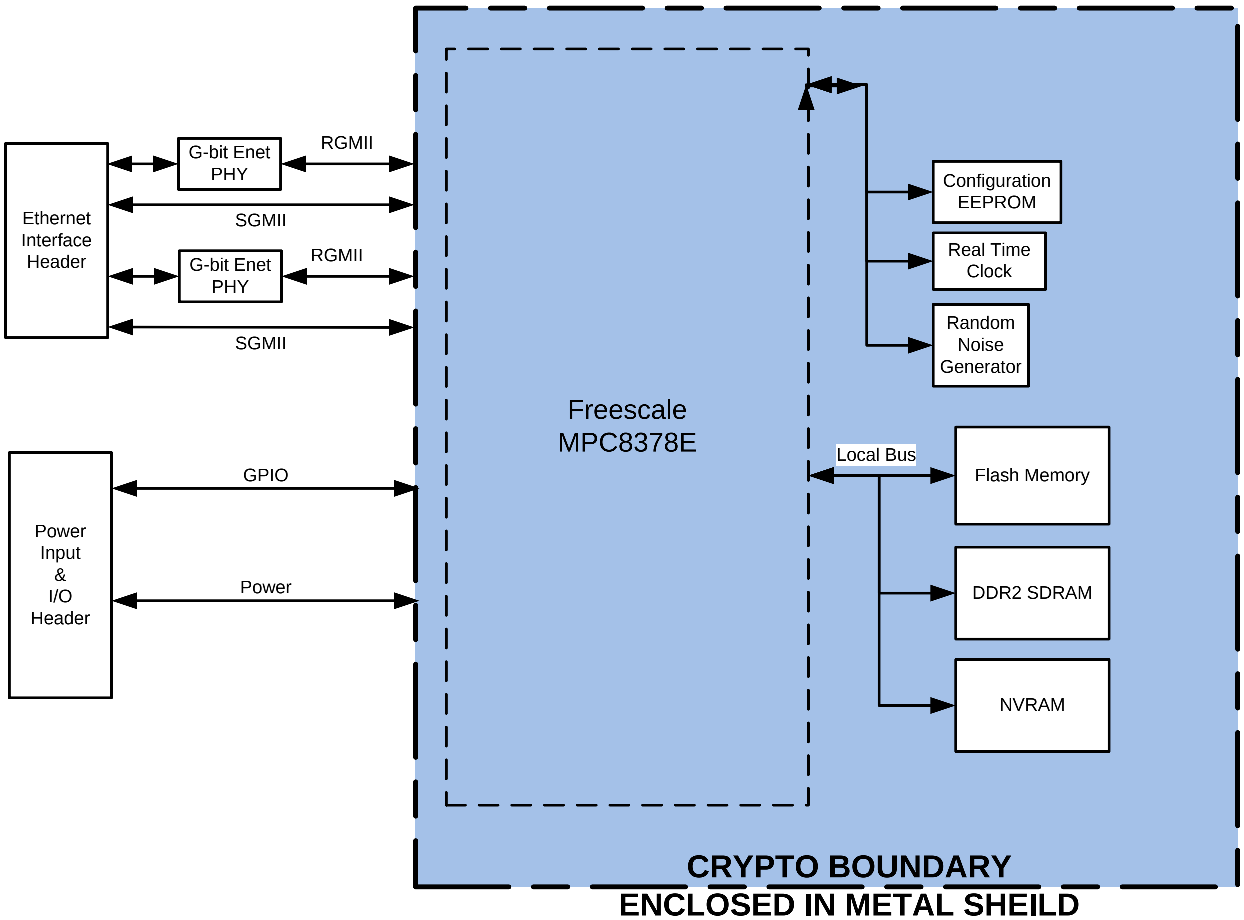

Figure 2 – Module High Level Block Diagram

The logical ports:

a. Status output: Ethernet port pins and GPIO (LED) connector pins
b. Data output: Ethernet port pins
c. Data input: Ethernet port pins
d. Control input: Ethernet port pins and RESET pin
e. Power input pin

3. Roles, Services, and Authentication

3.1 Roles & Services

The module supports the following authorized roles for operators.

3e-local Role: This role performs all security functions provided by the module. This role performs cryptographic initialization and management functions (e.g., module initialization, input/output of cryptographic keys and SRDIs, audit functions and user management). The 3e-local with default user (3e-CryptoOfficer) authenticates to the module using a username and password. 3e-local Role is responsible for managing (creating, deleting) Administrator users.

3e-CryptoOfficer Role: This role inherits all 3e-local privileges except the ability to create and manage users locally and configure module's Remote A&A settings.

3e-Administrator Role: This role performs general module configuration. No security management functions are available to the Administrator. The Administrator can also reboot the module if deemed necessary. The Administrator authenticates to the module using a username and password. All Administrators are identical, i.e., they have the same set of services available.

End User role: The End User role can set up VPN tunnel using IKEv2 to the module and send or receive data to and from the module. The End User role can also use VLAN encryption service of the module. End User Role can only use the cryptographic service but can't configure the device. The End User role is authenticated via its digital certificate and its knowledge of the corresponding private key.

The following table describes the module's services, including purpose and functions, and the details about the service:

Table 2: Services and User Access

Service and Purpose	Details	3e-local/ 3e-CryptoOfficer	3e-Administrator	End User	CSP Access (CSP ID table 6)
Input of Keys	IKE v2 digital certificate private key, VLAN encryption key, 802.1X supplicant private key, device HTTPS private keys, authentication key with RADIUS server SNMPv3 encryption key	X			3,15,16,19,20,21,22,23,33,23,24,25,26,37
Create and manage Administrator user	Support up to 5 administrator users	X			1
Change password	Administrator change his own password only	X	X		1
Show system status	View traffic status and systems log excluding security audit log	X	X		None

Security Audit Log	View & configure settings	X			None
System log	View & configure settings	X	X		None
Key zeroization via reboot		X	X		None
Factory default	Delete all configurations and set device back to factory default state	X			None
Perform Self-Test	Run algorithm KAT	X	X		None
Load New Firmware	Upload Ultra digital signed firmware	X			2,5
SNMP Management	All SNMP setting including SNMPv3 encryption key	X	X		3
HTTPS Management	Load HTTPS server certificate, private key	X			23,24,32,33
IPSec data encryption & decryption				X	9,10,11,12,13,14,15,16,17,18
VLAN data encryption & decryption				X	19,20

The table below shows the services and their access rights to the Critical Security Parameters (CSPs):

Table 3- CSPs and Access by Services

Service and Purpose	CSPs	Access
Input of Keys	IKE v2 digital certificate private key, 802.1X supplicant private key, device HTTPS private keys, authentication key with RADIUS server	Write
Create and manage Administrator user	Administrator Password	Read and Write
Change password	Crypto Officer, Administrator password	Read and Write
Show system status	None	None
Key zeroization via reboot	All	Write
Factory default	Delete all configurations and set device back to factory default state, zeroize all CSPs	Write
Perform Self-Test	None	None
IPSec data encryption & decryption	IPSec ESP session keys	Execute
VLAN data encryption & decryption	VLAN encryption keys	Execute
Load new firmware	Firmware signing public key	Read
HTTPS management	HTTPS server certificate, private key	Read

3.2 Authentication Mechanisms and Strength

The following table identifies the strength of authentication for each authentication mechanism supported:

Table 4: Identity Based Authentication & Strength of Authentication

Role	Authentication Mechanism	Strength of Mechanism
3e-local	Username and password	(8-30 chars) Minimum 8 characters => 1:94^8 = 1.641E
3e-CryptoOfficer	Username and password	(8-30 chars) Minimum 8 characters => 1:94^8 = 1.641E-16
3e-Administrator	Username and password	(8-30 chars) Minimum 8 characters => 1:94^8 = 1.641E-16
End User	RSA/ ECDSA certificate, Static AES key for VLAN	2048/3072 bits key (RSA), 256/384/521 bits key for ECDSA 128/192/256 bits AES key

The module halts (introduces a delay) for one second after each unsuccessful authentication attempt by *3e-CryptoOfficer* or *3e-Administrator*. The highest rate of authentication attempts to the module is one attempt per second. This translates to 60 attempts per minute. Therefore the probability for multiple attempts to use the module's authentication mechanism during a one-minute period is 60/(94^8), or less than (9.84E-15).

Using conservative estimates and equating a 2048 bits RSA key to a 112 bits symmetric key, or 256 bits ECDSA key equating 128 bits symmetric key, the probability for a random attempt to succeed is $1:2^{112}$. The fastest network connection supported by the module is 1 Gbps. Hence at most ($1 \times 10^9 \times 60 = 6 \times 10^{10}$) 60,000,000,000 bits of data can be transmitted in one minute. The number of possible attacks per minute is $6 \times 10^{10}/112$. Therefore, the probability that a random attempt will succeed, or a false acceptance will occur in one minute, is less than 1: (2^{112} x112/ 60×10^9), which is less than 100,000 as required by FIPS 140-2. For VLAN encryption *end user*, the static AES key with 128/192/256 bits offers the equivalent or stronger authentication strength.

4. Operational Environment

The module is a hardware module. The module’s operating system is a nonmodifiable operating system. Thus, the requirements from FIPS 140-2, section 4.6.1, are not applicable to the module.

5. Cryptographic Algorithms

The module supports the following FIPS-approved cryptographic algorithms. The algorithms are listed below, along with their corresponding CAVP certificate numbers.

The module implements SP800-90B compliant entropy source ENT (P). The entropy source falls into IG 7.14, Scenario #1a: A hardware module with an entropy-generating ENT (P) inside the module’s cryptographic boundary. The hardware-based entropy source provides at least 256 bits of entropy to seed SP800-90a DRBG for the use of key generation. The module produces raw entropy at about 17K bits/sec with a conservative estimation of 6 bits of entropy per byte from the raw source.

5.1 Approved Cryptographic Algorithms

Table 5 – FIPS Algorithms

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
Ultra MPC8378E Cryptographic Core					
A1701	AES	FIPS197, SP800-38A	CBC, ECB, GCM	128, 192, 256	Data Encryption/Decryption
A1701	HMAC	FIPS198-1, FIPS180-4	SHA-1, SHA2-224, SHA2-256	128	Keyed Hash
			SHA2-384,	192	
			SHA2-512	256	
A1701	Secure Hashing	FIPS180-4	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512		Secure Hashing
Ultra OpenSSL Algorithm Implementation					
A1702	AES	FIPS197, SP800-38A	ECB, CBC	128, 192, 256	Data Encryption/Decryption
A1702	DRBG	SP800-90A	AES-CTR	128, 192, 256	Deterministic Random Bit Generation
A1702	DRBG	SP800-90A	HMAC_DRBG	SHA1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	Deterministic Random Bit Generation **Tested by CAVP but not used by module*
A1702	DRBG	SP800-90A	Hash_DRBG	SHA2-224, SHA2-256, SHA2-384, SHA2-512	Deterministic Random Bit Generation **Tested by CAVP but not used by module*
ENT (P)		SP800-90B	TRNG		Entropy Generation
A1702	ECDSA	FIPS186-4	KeyGen, KeyVer, SigGen, SigVer	P-256, P-384, P-521	Digital Signature Generation and Verification. Key Generation and Verification
A1702	HMAC	FIPS198-1, FIPS180-4, FIPS202	SHA-1, SHA2-224, SHA2-256, SHA3-224, SHA3-256	128	Keyed Hash
			SHA2-384, SHA3-384	192	
			SHA2-512, SHA3-512	256	** SHA3 Tested by CAVP but not used by module*
A1702	Secure Hashing	FIPS180-4, FIPS202	SHA-1, SHA2-224, SHA2-256, SHA2-384,		Secure Hashing

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
			SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512		**SHA3 tested by CAVP but not used by module*
A1702	RSA	FIPS186-4	KeyGen, SigGen, SigVer	2048, 3072 for KeyGen, SigGen. 1024, 2048, 3072 for SigVer	Digital Signature Generation and Verification. Key Generation
A1702	CVL KDF	SP800-135rev1	TLS 1.2 SNMPv3, IKEv2		Key Derivation **TLS 1.0/1.1 Tested by CAVP but not used by module. No parts of TLS protocol other than KDF have been tested by CMVP/CAVP*
A1702	KAS-SSC (ECC/FFC)	SP800-56Arev3	KAS-ECC-SSC: ephemeralUnified: KAS Role: initiator, responder KAS-FFC-SSC: dhEphem: KAS Role: initiator, responder	KAS-ECC-SSC: P-256, P-384, P-521; KAS-FFC-SSC: ffdhe2048 and MODP-2048	KAS-ECC: Key establishment methodology provides between 128 and 256 bits of encryption strength KAS-FFC: Key establishment methodology provides 112 bits of encryption strength
A1702	KAS (ECC/FFC) KAS (KAS-SSC Cert. #A1702, CVL Cert. #A1702);	SP800-56Arev3; SP800-135rev1	KAS (ECC): ephemeralUnified: KAS Role: initiator, responder KAS (FFC): dhEphem: KAS Role: initiator, responder	KAS (ECC): P-256, P-384 and P-521 with IKEv2 KDF (SP800-135rev1); KAS (FFC): ffdhe2048, MODP-2048 with TLSv1.2 and IKEv2 KDF (SP800-135rev1)	Key Agreement Scheme per SP800-56Arev3 with key derivation function (SP800-135rev1) Note: The module's KAS (ECC/FFC) implementation is FIPS140-2 IG D.8 Scenario X1 (path 2) compliant
A1702	KTS	SP800-38F	AES-CBC with HMAC	AES-128, AES-196, AES-256	Key Wrapping/Unwrapping

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
N/A	CKG (Vendor affirmed)	SP800-133rev2			Cryptographic Key Generation as per section 6 in SP800-133rev2
Ultra Linux Kernel Cryptographic Library					
A2324	Secure Hashing	FIPS180-4	SHA2-256		Secure Hashing used in entropy conditioning

Notes:

- There are some algorithm modes that were tested but not used by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table.
- The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 7296 for IPSec/IKEv2. The module uses RFC 7296 compliant IKEv2 to establish the shared secret from which the AES GCM encryption keys are derived. The operations of one of the two parties involved in the IKE key establishment scheme shall be performed entirely within the cryptographic boundary of the module being validated. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.
- Use of a truncated HMAC-SHA-1-96 (HMAC Cert. #A1702) in SNMPv3 protocol is compliant to IG A.8.
- No parts of the TLS, SNMP and IPsec protocols, other than the KDFs, have been tested by the CAVP and CMVP.
- In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per section 6 in SP800-133rev2. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90A DRBG

5.2 Non-FIPS Approved Algorithms Allowed in FIPS Mode

The module supports the following non-FIPS approved algorithm which is permitted for use in the FIPS approved mode:

- RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)

6. Cryptographic Keys and SRDIs

All keys entered are encrypted using **HTTP over TLS** through the module's WebUI interface. Below is the Cryptographic Key and Security Relevant Data Item (SRDI) table:

Table 6: SRDI Table

Non-Protocol Keys/CSPs							
CSP ID	**Key/CSP**	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
1	Operator passwords	ASCII string	Input encrypted (using TLS session key)	Not output	PKCS5 hash in flash	Zeroized when reset to factory settings.	Used to authenticate CO and user role operators
2	Firmware verification key	ECDSA public key (256 bits)	Embedded in firmware at compile time. Firmware upgrade is through encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when firmware is upgraded.	Used for firmware digital signature verification
3	SNMP packet authentication keys, username	HMAC key (ASCII string, 128-256 bits)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	Zeroized when reset to factory settings.	Use for SNMP message authentication
4	SNMP packet encryption key	AES Key (HEX string) AES (128/192/256)	Internally derived by SNMP KDF	Not output	Plaintext in RAM	Zeroized when SNMP session terminated.	Use to encrypt SNMPv3 packet
5	system config AES key (256 bit)	AES key (HEX string)	Hardcoded in FLASH	Not output	Plaintext in FLASH	Zeroized when firmware is upgraded.	Used to encrypt the configuration file
	SP800-90A DRBG Keys/CSPs						
	Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
6	DRBG CTR V	32-byte value	32 bytes from /dev/random file, /dev/random is populated by hardware noise generator	Not output	Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS DRBG after it is used.	Used as CTR V value for FIPS DRBG.
7	DRBG CTR Key	32-byte value	32 bytes from /dev/random file, /dev/random is populated by hardware noise generator	Not output	Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS DRBG after it is used.	Used as CTR key for FIPS DRBG.
8	DRBG input string	48-byte value	Read from /dev/random	Not output	Plaintext in RAM	Zeroized every time a read operation on /dev/random.	Read by CTR_DRBG
	Ultra IPsec Protocol Keys/CSPs						
	Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
9	DH Private Key	224 bits	Generated	None	plaintext in RAM	Zeroized when no longer used	IKE v2 SA setup
10	DH Public Key	2048 bits	Generated	Output to peer	Plaintext in RAM	Zeroized when no longer used.	IKE v2 SA setup
11	ECCDH Private Key	P-256, P384, P-521 bits	Generated	None	Plaintext in RAM	Zeroized when no longer used	IKE v2 SA setup
12	ECCDH Public Key	P-256, P-384, P-521	Generated	Output to peer	Plaintext in RAM	Zeroized when no longer used.	IKE v2 SA setup

13	Peer DH Public Key	2048 bits	Input from peer as IKE protocol	Not output	plaintext in RAM	Zeroized when no longer used.	IKE v2 SA setup
14	Peer ECCDH Public Key	P-256, P-384, P-521	Input from peer as IKE protocol	Not output	Plaintext in RAM	Zeroized when no longer used.	IKE v2 SA setup
15	IPSec SA authenticatio n certificate private key	RSA (2048,3072) ECDSA (P-256, P-384, P-512)	Input encrypted (using TLS session key)	Not output	Plaintext in RAM and encrypted in FLASH	Flash copy At factory default RAM copy zeroized when not in use	IKE v2 SA authentication
16	IPSec IKE SA authenticatio n PSK	256 bits	Input encrypted (using TLS session key)	Not output	Plaintext in RAM and encrypted in flash	flash copy at factory default RAM copy zeroized when no longer used.	IKE v2 SA authentication
17	IPSec SA session key	AES (128/192/256)	Derived from DH/ECCDH key exchange	Not output	Plaintext in RAM	Zeroized when no longer used.	Encrypt and authenticate IKE v2 SA messages
18	IPSec ESP symmetric Data encryption key	AES/AES_GCM (128,192,256)	Not input (part of the KEYMAT that is established via IKE_AUTH)	Not output	Plaintext in RAM	Zeroized when child SA lifetime expired	Encrypt IPSec ESP data
	VLAN Data Encryption						
19	VLAN Data Encryption key (one per VLAN, up to 16 VLANs)	128/192/256 bits AES symmetric key	Input encrypted (using TLS session key)	Not output	Plaintext in RAM and encrypted in FLASH	Zeroized at factory default reset	Used to encrypt/decrypt data per VLAN
20	HMAC-SHA1 key	160 bits key	Input encrypted (using TLS session key)	Not output	Plaintext in RAM and encrypted in FLASH	Zeroized at factory default reset	Used to generate keyed digest for the encrypted VLAN data, adding integrity for AES ECB or CBC mode.
	3eTI Security Server Keys/CSPs (When Module is configured as 802.1X authenticator)						
	Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
21	Security Server password	HMAC key (ASCII string)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key", plain text in RAM	Zeroized at factory default reset	Authenticate module to Security Server in support of IPSec SA EAP-TLS authentication
	3eTI 802.1X Supplicant Keys/CSPs (when Module is configured as 802.1X supplicant)						
	Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
22	802.1X Supplicant private key	RSA (1024,2048, 3072) ECDSA (256,384,512)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	Zeroized at factory default reset	Used to authenticate with Authentication Server

	RFC 2818 HTTPS Keys/CSPs						
	Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
23	RSA private key	RSA (2048/3072) (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)	Installed at factory by default or installed by Crypto Officer via TLS or internally generated	Not output	Plaintext in flash	Zeroized when new private key is uploaded	Used to support CO and Admin HTTPS interfaces.
24	RSA public key	RSA (2048)	Installed at factory by default or installed by Crypto Officer via TLS or internally generated	Output to TLS client	Plaintext in flash	Zeroized when the web server certificate is deleted from certificate store and when firmware is upgraded.	Used to support CO and User HTTPS interfaces.
25	TLS DH private key	224 bits	Generated	Not output	Plaintext in RAM	Zeroized with the TLS session terminated	Used to support CO and User HTTPS interfaces.
26	TLS DH public key	2048 bits	Generated	Output to peer	Plaintext in RAM	Zeroized with the TLS session terminated.	Used to support CO and User HTTPS interfaces.
27	Peer TLS DH public key	2048 bits	Input from peer	Not output	Plaintext in RAM	Zeroized with the TLS session terminated	Used to support CO and User HTTPS interfaces.
28	TLS pre-master secret	48 bytes	Not input, derived using TLS protocol	Not output	Plaintext in RAM	Zeroized when session terminated.	Used to protect HTTPS session.
29	TLS master secret	48 bytes	Not input, derived from TLS pre-master secret	Not output	Plaintext in RAM	Zeroized when session terminated.	Used to protect HTTPS session.
30	TLS session key for encryption	AES (128/192/256)	Not input, derived using TLS protocol	Not output	Plaintext in RAM	Zeroized when a page of the web GUI is served after it is used.	Used to protect HTTPS session.
31	TLS session key for message authenticatio n	HMAC (128/192/256)	Not input, derived from TLS master secret	Not output	Plaintext in RAM	Zeroized when a page of the web GUI is served after it is used.	Used to protect HTTPS session.
	Public Security Parameter						
32	HTTPS Public certificate	RSA (2048/3072)	Input encrypted (using TLS session key)	During TLS session setup	Plaintext in flash	Zeroized when new certificate is loaded	Used to setup TLS session for HTTPS
33	HTTPS root certificate	RSA (2048/3072)	Input encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when new root certificate is loaded	Used to setup TLS session for HTTPS
34	IPSec Public certificate	RSA (2048,3072) ECDSA (256,384,512)	Input encrypted (using TLS session key)	During IPSec SA negotiation	Plaintext in flash	Zeroized when new certificate is loaded	Used for mutual authentication of the IPSec SA
35	IPSec Root certificate	RSA (2048,3072) ECDSA (256,384,512)	Input encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when new root certificate is loaded	Used for mutual authentication of the IPSec SA

36	802.1X supplicant public certificate	RSA (1024, 2048, 3072) Note: RSA 1024 bits key is used for digital signature verification, it's for legacy use per NIST SP800-131A	Input encrypted (using TLS session key)	During EAP-TLS session setup	Plaintext in flash	Zeroized when new certificate is loaded	authentication of the EAP-TLS
37	802.1X supplicant root certificate	RSA (1024,2048, 3072) Note: RSA 1024 bits key is used for digital signature verification, it's for legacy use per NIST SP800-131A	Input encrypted (using TLS session key)		Plaintext in flash	Zeroized when new root certificate is loaded	authentication of the EAP-TLS

7. Self-Tests

Ultra OpenSSL Power-On Self-Tests (POSTs):

- AES CBC 128/192/256 bit – encrypt/decrypt KAT
- AES ECB 128/192/256 bit – encrypt/decrypt KAT
- SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 KAT
- HMAC (SHA-1/SHA2-224/SHA2-256/SHA2-384/SHA2-512) KAT
- ECDSA Power On Self-Test (PWCT Sign and Verify)
- RSA sign/verify KATs (separate KAT for signing; separate KAT for verification)
- SP800-90A CTR_DRBG KAT
  (DRBG health tests per SP800-90A Section 11.3)
- SP800-135rev1 TLS 1.2 KDF KAT
- SP800-135rev1 SNMPv3 KDF KAT
- SP800-135rev1 IKEv2 KDF KAT
- KAS-ECC-SSC Primitive Z KAT
- KAS-FFC-SSC Primitive Z KAT

Firmware Integrity Test

- Firmware Integrity Test with ECDSA P-256 SHA2-256 verify
- Bootloader Integrity Test with ECDSA P-256 SHA2-256 verify

Ultra MPC8378E Cryptographic Core Power-on self-tests:

- AES CBC 128/192/256 – encrypt/decrypt KATs
- AES ECB 128/192/256 – encrypt/decrypt KATs
- AES GCM 128/192/256 – encrypt/decrypt KATs
- SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 KATs

- HMAC SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 KATs

ENT (P) SP800-90B Start-Up Health Tests:

- Repetition Count Test (RCT)
- Adaptive Proportion Test (APT)

Note: Please refer to SP800-90B, sections 4.4.1 and 4.4.2 for more information about the RCT and APT.

Ultra Linux Kernel 4.6 Cryptographic Library Power-On Self-Test:

- SHA2-256 KAT

After the module is powered on, the first thing done by bootloader is to check firmware integrity by verifying the digital signature of the firmware. If the integrity is broken, the firmware won't boot. Firmware integrity is also performed at POST during firmware boot up. The bootloader integrity is done at POST as well. Both firmware and bootloader are digitally signed with ECDSA.

The module performs SP800-90B compliant start-up health tests (RCT and APT) on ENT (P) output sequence (1024 consecutive samples) at power-on. Any entropy test failures will cause SYS_HALT.

Upon self-test failure, the module will go into the SYS_HALT state with failure messages written in the audit log and the Status LEDs pin set to high.

Conditional Self-Tests:

The module also performs the following conditional self-tests:

- ECDSA PWCT
- RSA PWCT
- KAS-FFC-SSC PWCT
- KAS-ECC-SSC PWCT
- Firmware Load Test (ECDSA with P-256 and SHA-256)
- ENT (P) SP800-90B Continuous Health Tests:
  - Repetition Count Test (RCT)
  - Adaptive Proportion Test (APT)

8. Physical Security Tamper Evidence

The physical security provided is intended to meet FIPS 140-2 Level 2 physical security (i.e. tamper evidence). The tamper evidence label (TEL) is applied at the factory. *3e-CryptoOfficer* should check the integrity of the label. If tampering evidence such as wrinkles, tears and marks on or around the label is found, the module shall not be used and it shall be returned to Ultra. The picture below shows the physical interface side of the module's enclosure with tamper-evident labels.

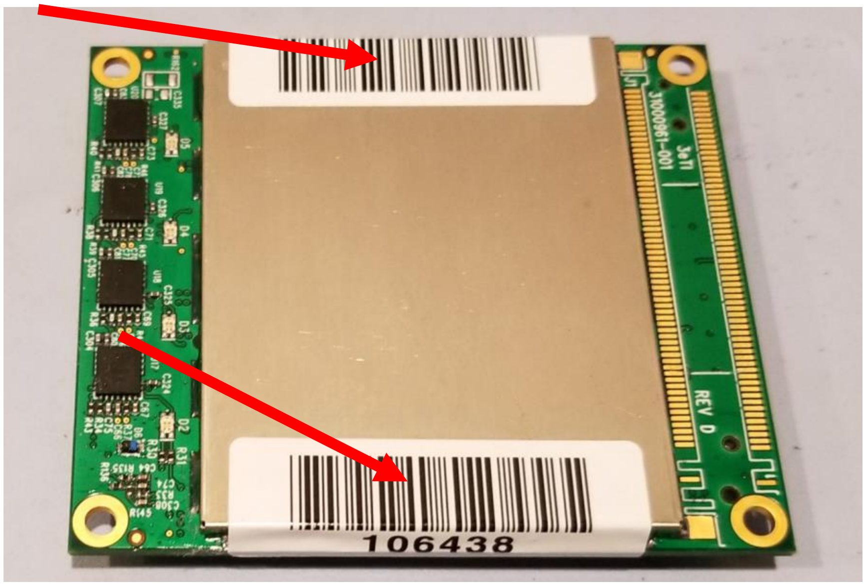

Figure 3 – Module Tamper Evidence Labels

Checking for Tamper Evidence

Tamper evidence tapes should be checked for nicks and scratches that make the metal case visible through the nicked or scratched seal.

Tamper Evidence Label (TEL) may show any of the following as evidence of tampering or removal:

- TEL is not preset in the positions prescribed (as shown above)
- TEL has been cut
- TEL is not stuck down well, or is loose
- Self-destruction of the TEL (broken bits or shreds) present as from an attempt of removal
- Tracking numbers do not match those recorded

In case of notification of tamper evidence, the 3*e-CryptoOfficer* shall not power on this module and shall contact 3eTI for factory repair.

9. Secure Rules & Configuration

Security Rules

The following module security rules must be followed by the operator in order to ensure secure operation:

1. The *3e-CryptoOfficer* shall not share any key or SRDI used by the module with any other operator or entity.
2. The *3e-CryptoOfficer* is responsible for inspecting the tamper evidence tapes. Other signs of tamper include wrinkles, tears and marks on or around the tape.
3. The *3e-CryptoOfficer* shall change the default password when configuring the module for the first time. The default password shall not be used. The module firmware also enforces the password change upon the *3e-CryptoOfficer*'s first log in.

4. The *3e-CryptoOfficer* shall login to make sure CSPs and keys are configured and applied in the module.
5. The *3e-CryptoOfficer* shall load the FIPS validated firmware only.

Security Configuration

The module operates in FIPS Approved Mode at all times. The *3e-CryptoOfficer* shall properly configure the module following the steps listed below:

1. Log in the module over HTTPS and change the default password (if this is the first time of use).
2. Configure the Management VPN tunnel with proper CSPs, such as certificate, private key, trust anchor and key expiration time.
3. Configure the Data VPN tunnel with proper CSPs, such as certificate, private key, trust anchor and key expiration time.
4. Configure the 802.1X supplication with proper CSPs, such as certificate, private key and trust anchor. (Optional)
5. *3e-CryptoOfficer* shall configure and setup the IPsec tunnel for data communication between the module and RADIUS server.

After configuration of the above items, reboot the device and the device will come back in full approved mode of operation.

10. Design Assurance

All source code and design documentation for this module is stored in version control system CVS. The module is coded in C with module's components directly corresponding to the security policy's rules of operation. Functional Specification is also provided.

The module is produced at Ultra's authorized manufactures only with CM being uniquely identified with a part number and the part number is under configuration management. Upon receiving a sales order with a verified customer, the part number together with shipping instructions is sent to manufacture. The manufacture builds and packs per instruction and generates a Traveler for each device which includes hardware and firmware versions per unit. The manufacture checks the label to ensure the unit matches with the purchase order before shipping. The end customer will examine the TEL upon receiving the unit and use the label's printed hardware/firmware version to match with the information displayed by the device's UI. The details of the procedure are covered by Ultra's ISO 9000 "Delivery Procedure" document.

11. Mitigation of Other Attack

The module does not mitigate other attack.