ULTRA

Ultra Intelligence and Communications

Edge Security Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

No table of figures entries found.

1 General

1.1 Overview

This is a non-proprietary cryptographic module security policy for the Ultra Intelligence & Communications Edge Security Cryptographic Module with firmware version 1.0 (hereinafter called ESM or the Module). The module is validated at the FIPS 140-3 overall level 2.

1.2 Security Levels

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	3
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module primarily acts as a network boundary protection device by using IPsec VPN or VLAN encryption services. Furthermore, it employs firewall and industrial control protocol packet inspection to provide defense-in-depth capabilities to prevent malicious attacks. The module offers Web GUI management via HTTPS using TLS v1.2 or TLS v1.3.

Module Type: Hardware

Module Embodiment: MultiChipEmbed

Module Characteristics:

Cryptographic Boundary:

The cryptographic boundary is defined as the entire chassis unit’s physical perimeter encompassing the "top," "front," "left," "right," “rear” and "bottom" surfaces of the case and shown in the figures below.

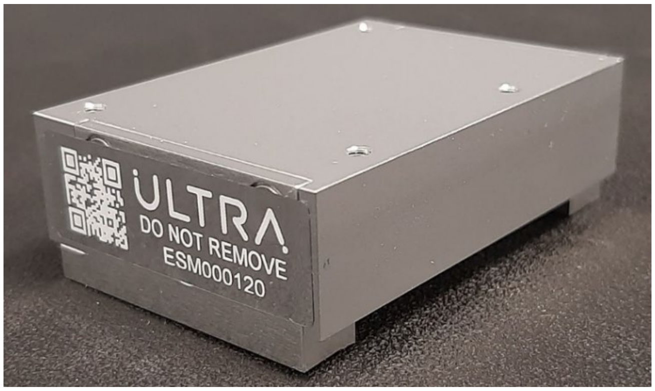


Figure 1: ESM Module Bottom

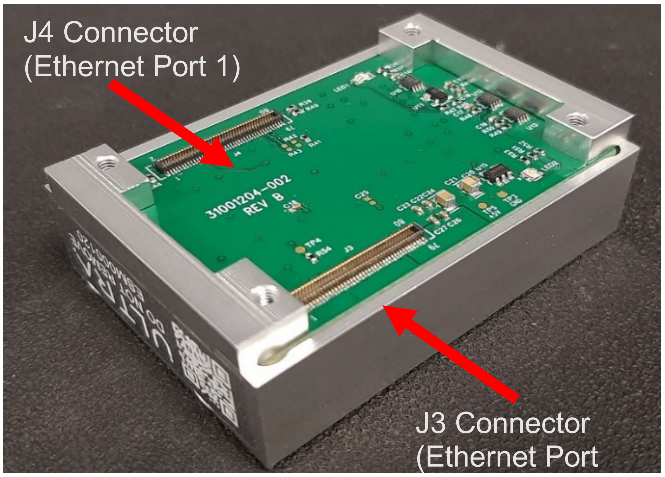


Figure 2: ESM Module Top

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Edge Security Model (ESM-110)	1.0	1.0	Marvell CN9130	N/A

Table 2: Tested Module Identification – Hardware

The module is a multiple-chip embedded hardware cryptographic module. The module's operational environment is limited. The module's firmware version is v1.0, and the module's hardware version is v1.0.

2.3 Excluded Components

The exposed electronic components (C16, R45, U11, C15, R46, R47, C18, C20, C21, C22, C23, C24, C27, R39, R40, R41, R44, R54 and TP4) in Figure 2 above are either capacitors or resistors associated with the power supply circuitry. They are excluded from the physical security requirements as they are only power supply circuitry related (non-security relevant).

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	The module is only operated in Approved mode of operation.	Approved	N/A

Table 3: Modes List and Description

The module is only operated in Approved mode of operation. The module doesn’t support non-approve mode or non-complaint state mode.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3316	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A3318	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A3316	Key Length - 128, 192, 256	SP 800-38C
AES-CCM	A3318	Key Length - 128, 192, 256	SP 800-38C
AES-ECB	A3316	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A3316	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	A3318	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
Counter DRBG	A3316	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - No	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A3316	Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3316	Component - No Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigVer (FIPS186-4)	A3316	Component - No Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512, SHA3-256, SHA3-384, SHA3-512	FIPS 186-4
HMAC-SHA-1	A3316	Key Length - Key Length: 128	FIPS 198-1
HMAC-SHA2-256	A3316	Key Length - Key Length: 128	FIPS 198-1
HMAC-SHA2-256	A3318	Key Length - Key Length: 128	FIPS 198-1
HMAC-SHA2-384	A3316	Key Length - Key Length: 192	FIPS 198-1
HMAC-SHA2-384	A3318	Key Length - Key Length: 192	FIPS 198-1
HMAC-SHA2-512	A3316	Key Length - Key Length: 256	FIPS 198-1
HMAC-SHA2-512	A3318	Key Length - Key Length: 256	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3316	Domain Parameter Generation Methods - P-256 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A3316	Domain Parameter Generation Methods - FB, FC, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF IKEv2 (CVL)	A3316	Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 224-8192 Increment 8 Derived Keying Material Length - Derived Keying Material Length: 1024-16384 Increment 8, Derived Keying Material Length: 384-16384 Increment 8 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF SNMP (CVL)	A3316	Password Length - Password Length: 64, 8192	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-4)	A3316	Key Generation Mode - B.3.3 Modulo - 2048, 3072 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A3316	Signature Type - PKCS 1.5 Modulo - 2048, 3072	FIPS 186-4
RSA SigVer (FIPS186-4)	A3316	Signature Type - PKCS 1.5 Modulo - 1024, 2048, 3072	FIPS 186-4
Safe Primes Key Generation	A3316	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
SHA-1	A3316	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A3316	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A3318	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A3316	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A3318	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A3316	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A3318	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A3316	Hash Algorithm - SHA2-256, SHA2-384	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A3316	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK, PSK-DHE	SP 800-135 Rev. 1

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	Ultra I&C OpenSSL	The cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per sections 4 and 5 in SP800-133rev2 (vendor affirmed) and FIPS 140-3 IG D.H. A seed (i.e., the random value) used in asymmetric key generation is a direct output from SP800-90Arev1 CTR_DRBG

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
KAS-ECC-KeyGen	KAS-KeyGen	KAS-ECC keypair generation		Counter DRBG
KAS-FFC-KeyGen	KAS-KeyGen	KAS-FFC keypair generation		Counter DRBG Safe Primes Key Generation
TLS KAS (ECC)	KAS-135KDF	KAS with TLSv1.2 KDF or TLSv1.3 KDF	Bit-strength Caveat:providing between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3 TLS v1.2 KDF RFC7627 TLS v1.3 KDF
TLS-KTS (AES-GCM)	KTS-Wrap	KTS wrap with AES-GCM	Bit-strength Caveat:providing between 128 and 256 bits of encryption strength	AES-GCM
TLS-KTS (AES and HMAC)	KTS-Wrap	KTS wrap with AES and HMAC	Bit-strength Caveat:providing between 128 and 256 bits of encryption strength	AES-CBC HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 SHA2-256 SHA2-384 SHA2-512
TLS RSA KeyGen	AsymKeyPair-KeyGen	RSA key gen		RSA KeyGen (FIPS186-4) keysize: 2048, 3072 Counter DRBG
TLS RSA SigGen	DigSig-SigGen	RSA SigGen		RSA SigGen (FIPS186-4) Keysize: 2048, 3072
TLS RSA SigVer	DigSig-SigVer	RSA SigVer		RSA SigVer (FIPS186-4) Keysize: 2048, 3072
IPSec/IKE KAS (ECC)	KAS-135KDF	KAS with IKEv2 KDF	Bit-strength Caveat:Providing between 128	KAS-ECC-SSC Sp800-

Name	Type	Description	Properties	Algorithms
			and 256 bits of encryption strength	56Ar3 KDF IKEv2
IPSec/IKE KAS (FFC)	KAS-135KDF	KAS with IKEv2 KDF	Bit-strength Caveat:Providing 112 bits of encryption strength	KAS-FFC-SSC Sp800-56Ar3 KDF IKEv2
IPSec/IKE ECDSA KeyGen	AsymKeyPair-KeyGen	ECDSA KeyGen		ECDSA KeyGen (FIPS186-4) Counter DRBG
IPSec/IKE ECDSA SigGen	DigSig-SigGen	ECDSA SigGen		ECDSA SigGen (FIPS186-4)
IPSec/IKE ECDSA SigVer	DigSig-SigVer	ECDSA SigVer		ECDSA SigVer (FIPS186-4)
IPSec/IKE RSA KeyGen	AsymKeyPair-KeyGen	RSA KeyGen		RSA KeyGen (FIPS186-4) Keysize: 2048, 3072 Counter DRBG
IPSec/IKE RSA SigGen	DigSig-SigGen	RSA SigGen		RSA SigGen (FIPS186-4) Keysize: 2048, 3072
IPSec/IKE RSA SigVer	DigSig-SigVer	RSA SigVer		RSA SigVer (FIPS186-4) keysize: 2048, 3072
IPSec Session Encrypt/Decrypt	BC-Auth BC-UnAuth	IPSec/IKEv2 session protection		AES-CBC AES-CCM AES-GCM AES-CBC AES-CCM AES-GCM
IPSec Session Authentication	MAC	IPSec Session Authentication		HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 SHA2-256

Name	Type	Description	Properties	Algorithms
				SHA2-384 SHA2-512 SHA2-256 SHA2-384 SHA2-512
SNMP Session Encrypt/Decrypt	BC-UnAuth	SNMPv3 Encryption/Decryption		AES-CBC
SNMP Session Authentication	MAC	SNMPv3 authentication		HMAC-SHA-1
VLAN Session Encrypt/Decrypt	BC-Auth BC-UnAuth	VLAN session encryption/decryption		AES-CBC AES-CCM AES-ECB
VLAN Session Authentication	MAC	VLAN session authentication		HMAC-SHA-1 HMAC-SHA2-256 SHA-1 SHA2-256
Firmware Load	AsymKeyPair-KeyVer	Firmware load test		RSA SigVer (FIPS186-4) keysize: 4096 SHA2-256
TLS Session Encrypt/Decrypt	BC-Auth BC-UnAuth	TLSv1.2/v1.3 Encryption/Decryption		AES-CBC AES-GCM
TLS Session Authentication	MAC	TLSv1.2/v1.3 session authentication		HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 SHA2-256 SHA2-384 SHA2-512
TLS Keying Materials Development	KAS-135KDF	TLS session keying materials, used to derive TLS session keys		TLS v1.2 KDF RFC7627 TLS v1.3 KDF
IPSec/IKE Keying Materials Development	KAS-135KDF	IPSec/IKE session keying materials, used to derive IPSec/IKE session keys		KDF IKEv2
SNMP Keying Materials Development	KAS-135KDF	SNMP session keying materials, used to derive SNMP session keys		KDF SNMP
DRBG Function	DRBG	DRBG generation		Counter DRBG

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in section 2.5.

Notes:

- No parts of the TLS, SNMP and IKE protocols, other than the KDFs, have been tested by the CAVP and CMVP.
- For TLSv1.2, the module's AES-GCM implementation conforms to FIPS 140-3 IG C.H scenario #1 following RFC 5288 for TLS. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP800-52 Rev1, Section 3.3.1. The operations of one of the two parties involved in the TLS key establishment scheme were performed entirely within the cryptographic boundary of the module being validated. The counter portion of the IV is set by the module within its cryptographic boundary. 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. The keys for the client and server negotiated in the TLSv1.2 handshake process (client_write_key and server_write_key) are compared and the module aborts the session if the key values are identical. 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.
- For TLS 1.3, the module offers the AES-GCM implementation and uses the context of Scenario #5 of FIPS 140-3 IG C.H. The protocol that provides this compliance is TLS 1.3, defined in RFC8446 of August 2018, using the ciphersuites that explicitly select AES-GCM as the encryption/decryption cipher (Appendix B.4 of RFC8446). The module supports acceptable AES-GCM ciphersuites from Section 3.3.1 of SP800-52rev2. The module implements, within its boundary, an IV generation unit for TLS 1.3 that keeps control of the 64-bit counter value within the AES-GCM IV. If the exhaustion condition is observed, the module will return an error indication to the calling application, who will then need to either trigger a re-key of the session (i.e., a new key for AES-GCM), or terminate the connection.
- In the event the module's power is lost and restored, the consuming application must ensure that new AES-GCM keys encryption or decryption under this scenario are established. TLS 1.3 provides session resumption, but the resumption procedure derives new AES-GCM encryption keys.
- The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED 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. Two keys established by IKEv2 for one security association (one key for encryption in each direction between the parties) are not identical and abort the session if they are. 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.

2.8 RBG and Entropy

Cert Number	Vendor Name
E109	Ultra Intelligence & Communications

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Ultra I&C Edge Security Module Entropy Source	Physical	Marvel 9130 CPU	8 bits	6.682	SHA2-256 (A3318)

Table 8: Entropy Sources

2.9 Key Generation

The module generates RSA, ECDSA, EC Diffie-Hellman, and Diffie-Hellman asymmetric key pairs compliant with FIPS 186-4, using a NIST SP 800-90Ar1 CTR DRBG for random number generation. In accordance with FIPS 140-3 IG D.H, the cryptographic module performs CKG for asymmetric keys as per section 5.1 of NIST SP 800-133rev2 (vendor affirmed) by obtaining a random bit string directly from an approved DRBG. The random bit string supports the required security strength requested by the calling application (without any V, as described in Additional Comments 2 of IG D.H).

2.10 Key Establishment

The module provides the following key/SSP establishment services in the approved mode of operation:

- KAS-FFC Shared Secret Computation:
    - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-FFC shared secret computation. The shared secret computation provides 112 bits of encryption strength.

- KAS-ECC Shared Secret Computation:
    - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-ECC shared secret computation. The shared secret computation provides between 128 and 256 bits of encryption strength.

2.11 Industry Protocols

The module supports TLS 1.2/1.3, SNMPv3 and IPsec/IKEv2. The module also supports VLAN encryption. The encryption uses AES ECB/CBC with HMAC, or AES-CCM with key size of 128 or 256 bits. Please refer to SSPs Table for more information.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Ethernet Port 1, Ethernet Port 2	Data Input	Data input into the module for all the services defined in Tables 8-11, including TLSv1.2, TLSv1.3, IPsec/IKEv2 and VLAN Encryption services data
Ethernet Port 1, Ethernet Port 2	Data Output	Data input into the module for all the services defined in Tables 8-11, including TLSv1.2, TLSv1.3, IPsec/IKEv2 and VLAN Encryption services data
Ethernet Port 1, Ethernet Port 2 and RESET PIN	Control Input	Control data input into the module for all the services defined in Tables 8-11, including TLSv1.2, TLSv1.3, IPsec/IKEv2 and VLAN Encryption services data. RESET Pin is used to send the control signal to reset the module
Ethernet Port 1, Ethernet Port 2 and GPIO status PIN	Status Output	Status Information output from the module

Table 9: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password-based Authentication	The minimum length is eight (8) characters (94 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is 1/(94^8) which is less than 1/1,000,000. As the module supports at most ten failed attempts to authenticate in a one-minute period, the probability of successfully	Password Based	The probability that a random attempt will succeed or a false acceptance will occur is 1/(94^8). Please refer to Description section in this table for more details	The probability of successfully authenticating to the module within one minute is 10/(94^8). Please refer to Description section in this table for more details

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	authenticating to the module within one minute is 10/(94^8), which is less than 1/100,000. This calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total.			
RSA-based Authentication	The modules support RSA public-key based authentication mechanism using a minimum of RSA 2048 bits, which provides 112 bits of security strength. The probability that a random attempt will succeed is 1/(2^112) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^112), which is less than 1/100,000.	RSA SigVer (FIPS186-4) (A3316)	The probability that a random attempt will succeed is 1/(2^112). Please refer to Description section in this table for more details	the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^112). Please refer to Description section in this table for more details

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
ECDSA-based Authentication	The modules support ECDSA public-key based authentication mechanism using a minimum of curve P-256, which provides 128 bits of security strength. The probability that a random attempt will succeed is 1/(2^128) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^128), which is less than 1/100,000.	ECDSA SigVer (FIPS186-4) (A3316)	The probability that a random attempt will succeed is 1/(2^128) which is less than 1/1,000,000. Please refer to Description section in this table for more details	the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^128). Please refer to Description section in this table for more details

Table 10: Authentication Methods

4.2 Roles

Name	Type	Operator Type	Authentication Methods
3e-Local	Identity	Crypto Officer	Password-based Authentication
3e-CryptoOfficer	Identity	Crypto Officer	Password-based Authentication
3e-Administrator	Identity	User	Password-based Authentication
End User	Identity	User	RSA-based Authentication ECDSA-based Authentication

Table 11: Roles

The module supports Identity-based authentication mechanism. Each entity is authenticated by the module upon initial access to the module. There are four roles supported by the module: 3e-Local (Role: Crypto Officer), 3e-CyrptoOfficer (Role: Crypto Officer), 3e-Administrator (Role: User) and End User (Role: User), as detailed below.

3e-Local: This role is defined as a Crypto Officer role and 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, audit functions and Operator account management). 3e-Local Role is responsible for managing (creating, deleting) 3e-CryptoOfficer role and 3e-Administrator role.

3e-CryptoOfficer: This role is defined as a Crypto Officer role and inherits all 3e-Local privileges except the ability to create and manage users locally.

3e-Administrator: This role is defined as a User 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: This role is defined as a User role and sets up VPN tunnel using IKEv2 to the module and send or receive data to and from the module. End User Role can only use the cryptographic service but cannot configure the device. The End User role is authenticated via its digital certificate and its knowledge of the corresponding private key.

The module does not support concurrent operator service.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Create User Account	Create User Accounts	N/A	Commands to create the other role's account	Status of the completion of account status	None	3e-Local - 3e-Local Password: W,Z - 3e-CryptoOfficer Password: W,Z - 3e-Administrator Password: W,Z
Configure Network	Commands to configure the network	N/A	Commands to configure the network	Status of the completion of network configuration status	None	3e-Local 3e-CryptoOfficer 3e-Administrator

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Status	Command used to show Module's Status	N/A	Command used to show Module's Status	Module's operational status	None	3e-Local 3e-CryptoOfficer 3e-Administrator
Show Version	Show module's ID and versioning information	N/A	Command to show Module's ID and version	Module's ID and versioning information	None	3e-Local 3e-CryptoOfficer 3e-Administrator
3e-Local Authentication	3e-Local role authentication	N/A	3e-Local authentication request	Status of the 3e-Local authentication	None	3e-Local - 3e-Local Password: W - 3e-Local Password: Z
3e-CryptoOfficer Authentication	3e-CryptoOfficer role authentication	N/A	3e-CryptoOfficer authentication request	Status of the 3e-CryptoOfficer authentication	None	3e-CryptoOfficer - 3e-CryptoOfficer Password: W,Z
3e-Administrator Authentication	3e-Administrator role authentication	N/A	3e-Administrator authentication request	Status of the 3e-Administrator authentication	None	3e-Administrator - 3e-Administrator Password: W,Z
End User Authentication	End User role authentication	N/A	End User authentication request	Status of the End User authentication	None	End User - IPSec/IKE Pre-shared Secret: W,Z
Perform Zeroization	Zeroize all SSPs	N/A	Command to zeroize the module	Status of the SSPs zeroization	None	3e-Local - DRBG Entropy Input: Z - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Seed: Z - DRBG Internal State V Value: Z - DRBG Key: Z - 3e-Local Password: Z - 3e-CryptoOfficer Password: Z - 3e-Administrator Password: Z - Firmware Load Test Key: Z - TLS ECDH Private Key: Z - TLS ECDH Public Key: Z - TLS Peer ECDH Public Key: Z - TLS ECDH Shared Secret: Z - TLS RSA Private Key: Z - TLS RSA Public Key: Z - TLS Master Secret: Z - TLS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Key: Z - TLS Authentication Key: Z - IPsec/IKE DH Private Key: Z - IPSec/IKE DH Public Key: Z - IPSec/IKE Peer DH Public Key: Z - IPSec/IKE DH Shared Secret: Z - IPSec/IKE ECDH Private Key: Z - IPSec/IKE ECDH Public Key: Z - IPSec/IKE Peer ECDH Public Key: Z - IPSec/IKE ECDH Shared Secret: Z - IPSec/IKE ECDSA Private Key: Z - IPSec/IKE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ECDSA Public Key: Z - IPSec/IKE RSA Private Key: Z - IPSec/IKE RSA Public Key: Z - IPSec/IKE Pre-shared Secret: Z - SKEYSEED: Z - IPSec/IKE Encryption Key: Z - IPSec/IKE Authentication Key: Z - SNMPv3 Shared Secret: Z - SNMPv3 Encryption Key: Z - SNMPv3 Authentication Key: Z - VLAN Encryption Key: Z - VLAN Authentication Key: Z 3e-CryptoOfficer - DRBG Entropy Input: Z - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Seed: Z - DRBG Internal State V Value: Z - DRBG Key: Z - 3e-Local Password: Z - 3e-CryptoOfficer Password: Z - 3e-Administrator Password: Z - Firmware Load Test Key: Z - TLS ECDH Private Key: Z - TLS ECDH Public Key: Z - TLS Peer ECDH Public Key: Z - TLS ECDH Shared Secret: Z - TLS RSA Private Key: Z - TLS RSA Public Key: Z - TLS Master Secret: Z - TLS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Key: Z - TLS Authentication Key: Z - IPsec/IKE DH Private Key: Z - IPSec/IKE DH Public Key: Z - IPSec/IKE Peer DH Public Key: Z - IPSec/IKE DH Shared Secret: Z - IPSec/IKE ECDH Private Key: Z - IPSec/IKE ECDH Public Key: Z - IPSec/IKE Peer ECDH Public Key: Z - IPSec/IKE ECDH Shared Secret: Z - IPSec/IKE ECDSA Private Key: Z - IPSec/IKE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ECDSA Public Key: Z - IPSec/IKE RSA Private Key: Z - IPSec/IKE RSA Public Key: Z - IPSec/IKE Pre-shared Secret: Z - SKEYSEED: Z - IPSec/IKE Encryption Key: Z - IPSec/IKE Authentication Key: Z - SNMPv3 Shared Secret: Z - SNMPv3 Encryption Key: Z - SNMPv3 Authentication Key: Z - VLAN Encryption Key: Z - VLAN Authentication Key: Z
Perform Self-Test	Perform self-tests	Self-Test service completion status	Command to trigger self-tests	Status of the self-tests results	None	3e-Local 3e-CryptoOfficer
Firmware Update	Perform firmware update	Firmware update service	Command to trigger	Status of the updated	Firmware Load	3e-Local - Firmware Load Test

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		completion status	firmware update	firmware installation		Key: R,E 3e-CryptoOfficer - Firmware Load Test Key: R,E
Configure TLS (v1.2/v1.3) Function	Configure TLS (v1.2/v1.3) Function	TLS configuration completion status	Commands to configure TLS (v1.2/v1.3)	Status of the completion of TLS (v1.2/v1.3) configuration	KAS-ECC-KeyGen TLS KAS (ECC) TLS-KTS (AES-GCM) TLS-KTS (AES and HMAC) TLS RSA KeyGen TLS RSA SigGen TLS RSA SigVer TLS Session Encrypt/Decrypt TLS Session Authentication TLS Keying Materials Development DRBG Function	3e-Local - DRBG Entropy Input: W,Z - DRBG Seed: W,Z - DRBG Internal State V Value: W,Z - DRBG Seed: W,Z - DRBG Internal State V Value: W,Z - DRBG Key: W,Z - TLS ECDH Private Key: W,Z - TLS ECDH Public Key: W,Z - TLS Peer ECDH Public Key: W,Z - TLS ECDH Shared Secret: W,Z - TLS RSA Private Key: W,Z - TLS RSA Public Key: W,Z - TLS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Master Secret: W,Z - TLS Encryption Key: W,Z - TLS Authentication Key: W,Z 3e-CryptoOfficer - DRBG Entropy Input: W,Z - DRBG Seed: W,Z - DRBG Internal State V Value: W,Z - DRBG Seed: W,Z - DRBG Internal State V Value: W,Z - DRBG Key: W,Z - TLS ECDH Private Key: W,Z - TLS ECDH Public Key: W,Z - TLS Peer ECDH Public Key: W,Z - TLS ECDH Shared Secret: W,Z - TLS RSA Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: W,Z - TLS RSA Public Key: W,Z - TLS Master Secret: W,Z - TLS Encryption Key: W,Z - TLS Authentication Key: W,Z
Configure SNMPv3 Function	Configure SNMPv3 Function	SNMPv3 configuration completion status	Commands to configure SNMPv3	Status of the completion of SNMPv3 configuration	SNMP Session Encrypt/Decrypt SNMP Session Authentication SNMP Keying Materials Development	3e-Local - SNMPv3 Shared Secret: W,Z - SNMPv3 Encryption Key: W,Z - SNMPv3 Authentication Key: W,Z 3e-CryptoOfficer - SNMPv3 Shared Secret: W,Z - SNMPv3 Encryption Key: W,Z - SNMPv3 Authentication Key: W,Z
Configure IPsec/IKEv2 Function	Configure IPsec/IKEv2 Function	IPsec/IKEv2 configuration completion status	Commands to configure IPsec/IKEv2	Status of the completion of IPsec/IKEv2 configuration	KAS-ECC-KeyGen KAS-FFC-KeyGen IPSec/IKE KAS (ECC) IPSec/IKE KAS (FFC)	3e-Local - IPsec/IKE DH Private Key: W,Z - IPSec/IKE DH Public Key: W,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					IPSec/IKE ECDSA KeyGen IPSec/IKE ECDSA SigGen IPSec/IKE ECDSA SigVer IPSec/IKE RSA KeyGen IPSec/IKE RSA SigGen IPSec/IKE RSA SigVer IPSec Session Encrypt/Decrypt IPSec Session Authentication IPSec/IKE Keying Materials Development DRBG Function	- IPSec/IKE Peer DH Public Key: W,Z - IPSec/IKE DH Shared Secret: W,Z - IPSec/IKE ECDH Private Key: W,Z - IPSec/IKE ECDH Public Key: W,Z - IPSec/IKE Peer ECDH Public Key: W,Z - IPSec/IKE ECDH Shared Secret: W,Z - IPSec/IKE ECDSA Private Key: W,Z - IPSec/IKE ECDSA Public Key: W,Z - IPSec/IKE RSA Private Key: W,Z - IPSec/IKE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						RSA Public Key: W,Z - IPSec/IKE Pre-shared Secret: W,Z - SKEYSEED: W,Z - IPSec/IKE Encryption Key: W,Z - IPSec/IKE Authentication Key: W,Z - DRBG Entropy Input: W,Z - DRBG Seed: W,Z - DRBG Internal State V Value: W,Z - DRBG Key: W,Z 3e-CryptoOfficer - IPsec/IKE DH Private Key: W,Z - IPSec/IKE DH Public Key: W,Z - IPSec/IKE Peer DH Public Key: W,Z - IPSec/IKE DH Shared Secret:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,Z - IPSec/IKE ECDH Private Key: W,Z - IPSec/IKE ECDH Public Key: W,Z - IPSec/IKE Peer ECDH Public Key: W,Z - IPSec/IKE ECDH Shared Secret: W,Z - IPSec/IKE ECDSA Private Key: W,Z - IPSec/IKE ECDSA Public Key: W,Z - IPSec/IKE RSA Private Key: W,Z - IPSec/IKE RSA Public Key: W,Z - IPSec/IKE Pre-shared Secret: W,Z - SKEYSEE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						D: W,Z - IPSec/IKE Encryption Key: W,Z - IPSec/IKE Authentication Key: W,Z - DRBG Entropy Input: W,Z - DRBG Seed: W,Z - DRBG Internal State V Value: W,Z - DRBG Key: W,Z
Configure VLAN Encryption	Configure VLAN Encryption	VLAN Encryption configuration completion status	Commands to configure VLAN Encryption	Status of the completion of VLAN Encryption configuration	VLAN Session Encrypt/Decrypt VLAN Session Authentication	3e-Local - VLAN Encryption Key: W,Z - VLAN Encryption Key: W,Z 3e-CryptoOfficer - VLAN Encryption Key: W,Z - VLAN Encryption Key: W,Z
Run TLS (v1.2/v1.3) Function	Run TLS (v1.2/v1.3) Function	TLSv1.2/1.3 service completion status	Initiate TLSv1.2 tunnel establishment request	Status of TLSv1.2 tunnel establishment	KAS-ECC-KeyGen TLS KAS (ECC) TLS-KTS (AES-GCM) TLS-KTS (AES and HMAC) TLS RSA KeyGen TLS RSA	3e-Local - DRBG Entropy Input: W,Z - DRBG Seed: W,Z - DRBG Internal State V Value: W,Z - DRBG Seed: W,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SigGen TLS RSA SigVer TLS Session Encrypt/Decrypt TLS Session Authentication TLS Keying Materials Development DRBG Function	- DRBG Internal State V Value: W,Z - DRBG Key: W,Z - TLS ECDH Private Key: W,Z - TLS ECDH Public Key: W,Z - TLS Peer ECDH Public Key: W,Z - TLS ECDH Shared Secret: W,Z - TLS RSA Private Key: W,Z - TLS RSA Public Key: W,Z - TLS Master Secret: W,Z - TLS Encryption Key: W,Z - TLS Authentication Key: W,Z 3e-CryptoOfficer - DRBG Entropy Input: W,Z - DRBG Seed: W,Z - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Internal State V Value: W,Z - DRBG Seed: W,Z - DRBG Internal State V Value: W,Z - DRBG Key: W,Z - TLS ECDH Private Key: W,Z - TLS ECDH Public Key: W,Z - TLS Peer ECDH Public Key: W,Z - TLS ECDH Shared Secret: W,Z - TLS RSA Private Key: W,Z - TLS RSA Public Key: W,Z - TLS Master Secret: W,Z - TLS Encryption Key: W,Z - TLS Authentication Key: W,Z 3e-Administrator - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Entropy Input: W,Z - DRBG Seed: W,Z - DRBG Seed: W,Z - DRBG Internal State V Value: W,Z - DRBG Key: W,Z - TLS ECDH Private Key: W,Z - TLS ECDH Public Key: W,Z - TLS Peer ECDH Public Key: W,Z - TLS ECDH Shared Secret: W,Z - TLS RSA Private Key: W,Z - TLS RSA Public Key: W,Z - TLS Master Secret: W,Z - TLS Encryption Key: W,Z - TLS Authentication Key: W,Z
Run SNMPv3 Function	Run SNMPv3 Function	SNMPv3 service	Initiate SNMPv3 tunnel	Status of SNMPv3 tunnel	SNMP Session Encrypt/Dec	3e-Local - SNMPv3 Shared

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		completion status	establishment request	establishment	rypt SNMP Session Authentication SNMP Keying Materials Development	Secret: W,Z - SNMPv3 Encryption Key: W,Z - SNMPv3 Authentication Key: W,Z 3e-CryptoOfficer - SNMPv3 Shared Secret: W,Z - SNMPv3 Encryption Key: W,Z - SNMPv3 Authentication Key: W,Z 3e-Administrator - SNMPv3 Shared Secret: W,Z - SNMPv3 Encryption Key: W,Z - SNMPv3 Authentication Key: W,Z
Run IPsec/IKEv2 Function	Run IPsec/IKEv2 Function	IPsec/IKEv2 service completion status	Initiate IPsec/IKEv2 tunnel establishment request	Status of IPSec/IKEv2 tunnel establishment	KAS-ECC-KeyGen KAS-FFC-KeyGen IPSec/IKE KAS (ECC) IPSec/IKE KAS (FFC) IPSec/IKE ECDSA KeyGen IPSec/IKE	3e-Local - IPsec/IKE DH Private Key: W,Z - IPSec/IKE DH Public Key: W,Z - IPSec/IKE Peer DH Public Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					ECDSA SigGen IPSec/IKE ECDSA SigVer IPSec/IKE RSA KeyGen IPSec/IKE RSA SigGen IPSec/IKE RSA SigVer IPSec Session Encrypt/Decrypt IPSec Session Authentication IPSec/IKE Keying Materials Development DRBG Function	W,Z - IPSec/IKE DH Shared Secret: W,Z - IPSec/IKE ECDH Private Key: W,Z - IPSec/IKE ECDH Public Key: W,Z - IPSec/IKE Peer ECDH Public Key: W,Z - IPSec/IKE ECDH Shared Secret: W,Z - IPSec/IKE ECDSA Private Key: W,Z - IPSec/IKE ECDSA Public Key: W,Z - IPSec/IKE RSA Private Key: W,Z - IPSec/IKE RSA Public Key: W,Z - IPSec/IKE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Pre-shared Secret: W,Z - SKEYSEED: W,Z - IPSec/IKE Encryption Key: W,Z - IPSec/IKE Authentication Key: W,Z - DRBG Entropy Input: W,Z - DRBG Seed: W,Z - DRBG Internal State V Value: W,Z - DRBG Key: W,Z 3e-CryptoOfficer - IPsec/IKE DH Private Key: W,Z - IPSec/IKE DH Public Key: W,Z - IPSec/IKE Peer DH Public Key: W,Z - IPSec/IKE DH Shared Secret: W,Z - IPSec/IKE ECDH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: W,Z - IPSec/IKE ECDH Public Key: W,Z - IPSec/IKE Peer ECDH Public Key: W,Z - IPSec/IKE ECDH Shared Secret: W,Z - IPSec/IKE ECDSA Private Key: W,Z - IPSec/IKE ECDSA Public Key: W,Z - IPSec/IKE RSA Private Key: W,Z - IPSec/IKE RSA Public Key: W,Z - IPSec/IKE Pre-shared Secret: W,Z - SKEYSEED: W,Z - IPSec/IKE Encryption

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: W,Z - IPSec/IKE Authentication Key: W,Z - DRBG Entropy Input: W,Z - DRBG Seed: W,Z - DRBG Internal State V Value: W,Z - DRBG Key: W,Z 3e-Administrator - IPsec/IKE DH Private Key: W,Z - IPSec/IKE DH Public Key: W,Z - IPSec/IKE Peer DH Public Key: W,Z - IPSec/IKE DH Shared Secret: W,Z - IPSec/IKE ECDH Private Key: W,Z - IPSec/IKE ECDH Public Key: W,Z - IPSec/IKE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Peer ECDH Public Key: W,Z - IPSec/IKE ECDH Shared Secret: W,Z - IPSec/IKE ECDSA Private Key: W,Z - IPSec/IKE ECDSA Public Key: W,Z - IPSec/IKE RSA Private Key: W,Z - IPSec/IKE RSA Public Key: W,Z - IPSec/IKE Pre-shared Secret: W,Z - SKEYSEED: W,Z - IPSec/IKE Encryption Key: W,Z - IPSec/IKE Authentication Key: W,Z - DRBG Entropy Input: W,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Seed: W,Z - DRBG Internal State V Value: W,Z - DRBG Key: W,Z
Run VLAN Encryption	Run VLAN Encryption	VLAN Encryption service completion status	Initiate VLAN Encryption tunnel establishment request	Status of VLAN Encryption tunnel establishment	VLAN Session Encrypt/Decrypt VLAN Session Authentication	3e-Local - VLAN Encryption Key: W,Z - VLAN Encryption Key: W,Z 3e-CryptoOfficer - VLAN Encryption Key: W,Z - VLAN Encryption Key: W,Z 3e-Administrator - VLAN Encryption Key: W,Z - VLAN Encryption Key: W,Z

Table 12: Approved Services

4.5 External Software/Firmware Loaded

The module also supports the firmware load test by using RSA 4096 bits with SHA2-256 (RSA Cert. #A3316) for the new validated firmware to be uploaded into the module. A Firmware Load Test Key was preloaded to the module's binary at the factory and used for firmware load test. In order to load new firmware, the Crypto Officer must authenticate to the module before loading the firmware. This ensures that unauthorized access and use of the module is not performed. The module will load the new update upon reboot. The update attempt will be rejected if the verification fails. Any firmware loaded into the module that is not shown on the module certificate, is out of scope of this validation and requires a separate FIPS 140-3 validation.

4.6 Additional Information

The module supports Unauthenticated service, where the unauthenticated users can run the self-test service by power-cycling the module.

5 Software/Firmware Security

5.1 Integrity Techniques

The module is provided in the form of binary executable code (Module's binary file name?). To ensure the software security, the module is digitally signed with RSA 4096 bits with SHA2-256 (RSA Cert. #3316) during the Pre-Operational Self-Test. A Firmware Integrity Test Key (non-SSP) was preloaded to the module's binary at the factory and used for firmware integrity test only at the pre-operational self-test. The module uses the RSA 4096 bits modulus public key to verify the digital signature. If the firmware integrity test fails, the module would enter to an Error state with all crypto functionality inhibited.

5.2 Initiate on Demand

Integrity test is performed as part of the Pre-Operational Self-Tests. It is automatically executed at power-on. The authorized operator can initiate the firmware integrity test on-demand via Web GUI's reboot command or power cycling.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

Not Applicable as the module is operated in a limited modifiable operational environments and the physical security (section 7) is level 2. The module's Operational Environment is limited as the module implements the firmware load service to support necessary updates.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper Evidence Seals	90 days	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

Mechanism	Inspection Frequency	Inspection Guidance
		an attempt of removal; Tracking numbers do not match those recorded. In addition, Please note that the TELs are not orderable. Please contact support@ultra-3eti.com for more information.

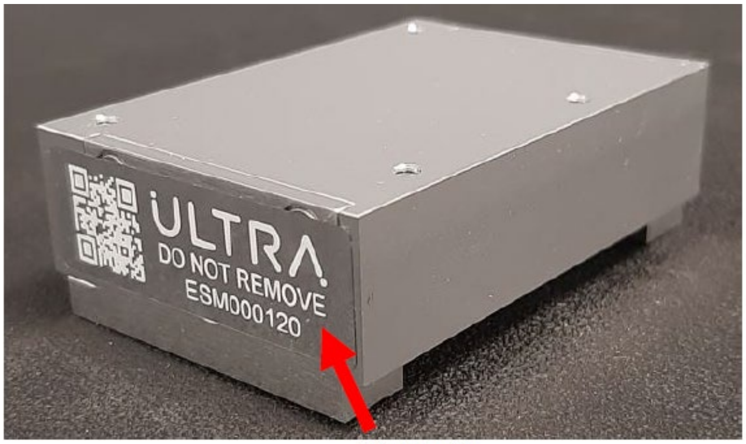
Table 13: Mechanisms and Actions Required

7.2 User Placed Tamper Seals

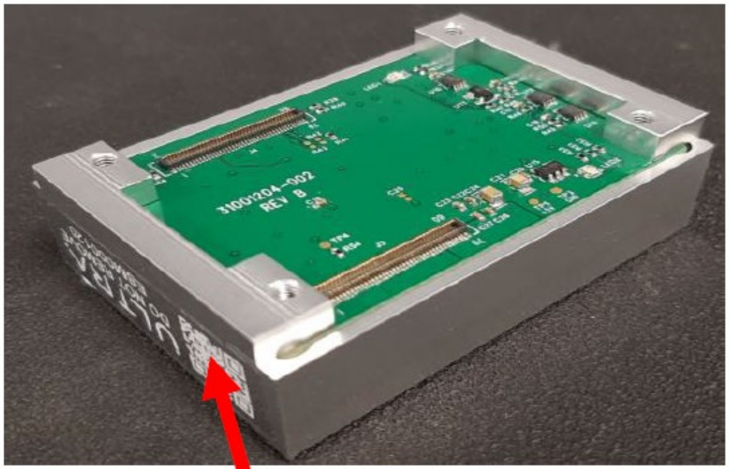
Two tamper evidence labels (TELs) are applied at Vendor’s factory, one on each side of the module. TELs are not orderable. Please contact support@ultra-3eti.com for more information.

Number: 2

Placement: Please refer to the TELs placement below.



TEL #1



TEL #2

Surface Preparation: N/A

Operator Responsible for Securing Unused Seals: N/A

Part Numbers: N/A

3e-CryptoOfficer is responsible for checking the integrity of the label by following the guidance listed above. In case of notification of tamper evidence, the 3e-CryptoOfficer shall not power on this module and shall contact 3eTI for factory repair. Any deviation of the TELs placement by unauthorized operators such as tearing, misconfiguration, removal, change, replacement or any other change in the TELs from its original configuration shall mean the module is no longer in the Approved mode of operation.

8 Non-Invasive Security

The module claims no non-invasive security techniques.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Volatile memory	Dynamic
Flash	Non-Volatile memory	Static

Table 14: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Module Public Key Output	Module	External (Outside the Module's Boundary)	Plaintext	Automated	Electronic	
Peer Public Key Input	External (Outside the Module's Boundary)	Module	Plaintext	Automated	Electronic	
Password/Secret Input encrypted by GCM	External (Outside the	Module	Encrypted	Automated	Electronic	TLS-KTS (AES-GCM)

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
	Module's Boundary)					
Password/Secret Input encrypted by AES and HMAC	External (Outside the Module's Boundary)	Module	Encrypted	Automated	Electronic	TLS-KTS (AES and HMAC)
VLAN SSPs Input via TLS-KTS (GCM)	External (Outside the Module's Boundary)	Module	Encrypted	Automated	Electronic	TLS-KTS (AES-GCM)
VLAN SSPs Input via TLS-KTS (AES and HMAC)	External (Outside the Module's Boundary)	Module	Encrypted	Automated	Electronic	TLS-KTS (AES and HMAC)

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroization command	CO issues zeroization service: "Factory Default" to zeroize all SSPs	The zeroization command will erase all SSPs stored in the RAM or in the Flash of the module.	Module Reboot
N/A	Zeroization requirements are not applicable	SSPs used solely for self-test purposes in module's self-test need not meet zeroization requirements	N/A

Table 16: SSP Zeroization Methods

1. The zeroization operations shall be performed under the control of the Crypto Officer role (3e-Local Role or 3e-CyrptoOfficer role).
2. To initiate zeroization, see Section End of Life / Sanitization in this document for more details.
3. The zeroized SSPs cannot be retrieved or reused. Once the command is initiated, the SSPs are overwritten with 0s.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Entropy Input	Used to seed the DRBG	384 bits - At least 256 bits	Entropy Inputs - CSP			DRBG Function
DRBG Seed	Used DRBG generation	256 bits - 256 bits	DRBG Seed - CSP			DRBG Function
DRBG Internal State V Value	Used for DRBG generation	256 bits - 256 bits	DRBG Internal State V Value - CSP			DRBG Function
DRBG Key	Used for DRBG generation	256 bits - 256 bits	DRBG Key - CSP			DRBG Function
3e-Local Password	Used for 3e-Local authentication	8-30 characters - N/A	Authentication Data - CSP			
3e-CryptoOfficer Password	Used for 3e-Local authentication	8-30 characters - N/A	Authentication Data - CSP			
3e-Administrator Password	Used for 3e-Administrator authentication	8-30 characters - N/A	Authentication Data - CSP			
Firmware Load Test Key	Used for firmware load test	4096 bits - 152 bits	Public Key - PSP			Firmware Load
TLS ECDH Private Key	TLS ECDH private key	Curves: P-256, P-384, P-512 - 128-256 bits	Private Key - CSP	KAS-ECC-KeyGen		TLS KAS (ECC)
TLS ECDH Public Key	TLS ECDH public key	Curves: P-256, P-384, P-512 - 128-256 bits	Public Key - PSP		KAS-ECC-KeyGen	TLS KAS (ECC)
TLS Peer ECDH Public Key	Used to derive TLS ECDH	Curves: P-256, P-384,	Public Key - PSP			TLS KAS (ECC)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Shared Secret	P-512 - N/A				
TLS ECDH Shared Secret	TLS ECDH shared secret	Curves: P-256, P-384, P-512 - 128-256 bits	Shared Secret - CSP		TLS KAS (ECC)	TLS KAS (ECC)
TLS RSA Private Key	Used for TLS peer authentication	Modulus: 2048 or 3072 bits - 112 or 128 bits	Private Key - CSP	TLS RSA KeyGen		TLS RSA SigGen
TLS RSA Public Key	Used for TLS peer authentication	Modulus: 2048 or 3072 bits - 112 or 128 bits	Public Key - PSP		TLS RSA KeyGen	TLS RSA SigVer
TLS Master Secret	Used to derive TLS Session keys	384 bits - 384 bits	TLS Master Secret - CSP		TLS Keying Materials Development	TLS Session Encrypt/Decrypt TLS Session Authentication
TLS Encryption Key	Used to protect TLS traffic confidentiality.	128-256 bits - 128-256 bits	Encryption Key - CSP		TLS Keying Materials Development	TLS Session Encrypt/Decrypt
TLS Authentication Key	Used to protect traffic confidentiality.	at least 112 bits - at least 112 bits	Authentication Key - CSP		TLS Keying Materials Development	TLS Session Authentication
IPsec/IKE DH Private Key	Used to derive IKE DH Shared Secret	MODP-2048 bits - 112 bits	Private Key - CSP	KAS-FFC-KeyGen		IPSec/IKE KAS (FFC)
IPSec/IKE DH Public Key	Used to derive IKE DH Shared Secret	MODP-2048 bits - 112 bits	Public Key - PSP		KAS-FFC-KeyGen	IPSec/IKE KAS (FFC)
IPSec/IKE Peer DH Public Key	Used to derive IKE	MODP-2048 - 112 bits	Public Key - PSP			IPSec/IKE KAS (FFC)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	DH Shared Secret					
IPSec/IKE DH Shared Secret	Used to derive IPSec/IKE Session Encryption Key and IPSec/IKE Authentication Key	MODP-2048 bits - 112 bits	Shared Secret - CSP		IPSec/IKE KAS (FFC)	IPSec/IKE KAS (FFC)
IPSec/IKE ECDH Private Key	Used to derive IKE ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128-256 bits	Private Key - CSP	KAS-ECC-KeyGen		IPSec/IKE KAS (ECC)
IPSec/IKE ECDH Public Key	Used to derive IKE ECDH Shared Secret	Curves: P-256, P-384, P-512 - 128-256 bits	Public Key - PSP		KAS-ECC-KeyGen	IPSec/IKE KAS (ECC)
IPSec/IKE Peer ECDH Public Key	Used to derive IKE ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128-256 bits	Public Key - PSP			IPSec/IKE KAS (ECC)
IPSec/IKE ECDH Shared Secret	Used to derive IKE ECDH Session Encryption Key and IPSec/IKE Authentication Key	Curves: P-256, P-384, P-521 - 128-256 bits	Shared Secret - CSP		IPSec/IKE KAS (ECC)	IPSec/IKE KAS (ECC)
IPSec/IKE ECDSA Private Key	Used for IPSec/IKE peer authentication	Curves: P-256, P-384, P-512 - 128-256 bits	Private Key - CSP	IPSec/IKE ECDSA KeyGen		IPSec/IKE ECDSA SigGen
IPSec/IKE ECDSA Public Key	Used for IPSec/IKE peer	Curves: P-256, P-384,	Public Key - PSP		KAS-ECC-KeyGen	IPSec/IKE ECDSA SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	authentication	P-512 - 128-256 bits				
IPSec/IKE RSA Private Key	Used for IPSec/IKE peer authentication	Modulus: 2048 or 3072 bits - 112 or 128 bits	Private Key - CSP	IPSec/IKE RSA KeyGen		IPSec/IKE RSA SigGen
IPSec/IKE RSA Public Key	Used for IPSec/IKE peer authentication	Modulus: 2048 or 3072 bits - 112 or 128 bits	Public Key - PSP		KAS-FFC-KeyGen	IPSec/IKE RSA SigGen
IPSec/IKE Pre-shared Secret	Used for IPSec/IKE peer authentication	16-32 bytes characters - N/A	Shared Secret - CSP			
SKEYSEED	Keying material used to derive the IPSec/IKE Session Encryption Key and IPSec/IKE Authentication Key	160 bits - N/A	Keying Material - CSP		IPSec/IKE Keying Materials Development	IPSec Session Encrypt/Decrypt IPSec Session Authentication
IPSec/IKE Encryption Key	Used to secure IPSec/IKEv2 traffic confidentiality	128-256 bits - 128-256 bits	Encryption Key - CSP		IPSec/IKE Keying Materials Development	IPSec Session Encrypt/Decrypt
IPSec/IKE Authentication Key	Used to secure IPSec/IKEv2 traffic integrity	At least 112 bits - At least 112 bits	Authentication Key - CSP		IPSec/IKE Keying Materials Development	IPSec Session Authentication
SNMPv3 Shared Secret	Used for SNMPv3 User authentication	8-32 characters - N/A	Authentication Secret - CSP			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SNMPv3 Encryption Key	Used to protect SNMPv3 traffic confidentiality	128 bits - 128 bits	Encryption Key - CSP		SNMP Keying Materials Development	SNMP Session Encrypt/Decrypt
SNMPv3 Authentication Key	Used to secure SNMPv3 traffic integrity	At least 112 bits - At least 112 bits	Authentication Key - CSP		SNMP Keying Materials Development	SNMP Session Authentication
VLAN Encryption Key	Used to protect VLAN data privacy	128 or 256 bits - 128 or 256 bits	Encryption Key - CSP			VLAN Session Encrypt/Decrypt
VLAN Authentication Key	Used to protect VLAN data integrity	At least 112 bits - At least 112 bits	Authentication Key - CSP			VLAN Session Authentication

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Entropy Input		RAM:Plaintext	Until Reboot	Zeroization command	DRBG Seed:Used With DRBG Internal State V Value:Used With DRBG Key:Used With
DRBG Seed		RAM:Plaintext	Until Reboot	Zeroization command	DRBG Entropy Input:Used With DRBG Internal State V Value:Used With DRBG Key:Used With
DRBG Internal State V Value		RAM:Plaintext	Until Reboot	Zeroization command	DRBG Entropy Input:Used With DRBG Seed:Used With DRBG Key:Used With
DRBG Key		RAM:Plaintext	Until Reboot	Zeroization command	DRBG Entropy Input:Used With DRBG Seed:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					DRBG Internal State V Value:Used With
3e-Local Password	Password/Secret Input encrypted by GCM Password/Secret Input encrypted by AES and HMAC	Flash:Encrypted	Until Reboot	Zeroization command	
3e-CryptoOfficer Password	Password/Secret Input encrypted by GCM Password/Secret Input encrypted by AES and HMAC	Flash:Encrypted	Until Reboot	Zeroization command	
3e-Administrator Password	Password/Secret Input encrypted by GCM Password/Secret Input encrypted by AES and HMAC	Flash:Encrypted	Until Reboot	Zeroization command	
Firmware Load Test Key		Flash:Plaintext	Until Reboot	N/A	
TLS ECDH Private Key		RAM:Plaintext	while TLS tunnel is on	Zeroization command	TLS ECDH Public Key:Paired With TLS Peer ECDH Public Key:Used With
TLS ECDH Public Key	Module Public Key Output	RAM:Plaintext	while TLS tunnel is on	Zeroization command	TLS ECDH Private Key:Paired With
TLS Peer ECDH Public Key	Peer Public Key Input	RAM:Plaintext	while TLS tunnel is on	Zeroization command	TLS ECDH Private Key:Used With
TLS ECDH Shared Secret		RAM:Plaintext	while TLS tunnel is on	Zeroization command	TLS ECDH Private Key:Derived From TLS Peer ECDH

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Public Key:Derived From
TLS RSA Private Key		Flash:Plaintext	while TLS tunnel is on	Zeroization command	TLS RSA Public Key:Paired With TLS Peer RSA Public Key:Used With
TLS RSA Public Key	Module Public Key Output	Flash:Plaintext	while TLS tunnel is on	Zeroization command	TLS RSA Private Key:Paired With
TLS Master Secret		RAM:Plaintext	while TLS tunnel is on	Zeroization command	TLS ECDH Shared Secret:Derived From
TLS Encryption Key		RAM:Plaintext	while TLS tunnel is on	Zeroization command	TLS Authentication Key:Used With
TLS Authentication Key		RAM:Plaintext	while TLS tunnel is on	Zeroization command	TLS Encryption Key:Used With
IPsec/IKE DH Private Key		RAM:Plaintext	while IPSec/IKE tunnel is on	Zeroization command	IPSec/IKE DH Public Key:Paired With
IPSec/IKE DH Public Key	Module Public Key Output	RAM:Plaintext	while IPSec/IKE tunnel is on	Zeroization command	IPsec/IKE DH Private Key:Paired With
IPSec/IKE Peer DH Public Key	Peer Public Key Input	RAM:Plaintext	while IPSec/IKE tunnel is on	Zeroization command	IPsec/IKE DH Private Key:Used With
IPSec/IKE DH Shared Secret		RAM:Plaintext	while IPSec/IKE tunnel is on	Zeroization command	SKEYSEED:Derive to
IPSec/IKE ECDH Private Key		RAM:Plaintext	while IPSec/IKE tunnel is on	Zeroization command	IPSec/IKE ECDH Public Key:Paired With IPSec/IKE Peer ECDH Public Key:Used With
IPSec/IKE ECDH Public Key	Module Public Key Output	RAM:Plaintext	while IPSec/IKE tunnel is on	Zeroization command	IPSec/IKE ECDH Private Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
IPSec/IKE Peer ECDH Public Key	Peer Public Key Input	RAM:Plaintext	while IPSec/IKE tunnel is on	Zeroization command	IPSec/IKE ECDH Private Key:Used With
IPSec/IKE ECDH Shared Secret		RAM:Plaintext	while IPSec/IKE tunnel is on	Zeroization command	SKEYSEED:Used With IPSec/IKE Encryption Key:Derived to IPSec/IKE Authentication Key:Derived to
IPSec/IKE ECDSA Private Key		Flash:Plaintext	while IPSec/IKE tunnel is on	Zeroization command	IPSec/IKE ECDSA Public Key:Paired With IPSec/IKE Peer ECDSA Public Key:Used With
IPSec/IKE ECDSA Public Key	Module Public Key Output	Flash:Plaintext	while IPSec/IKE tunnel is on	Zeroization command	IPSec/IKE ECDSA Private Key:Paired With
IPSec/IKE RSA Private Key		Flash:Plaintext	while IPSec/IKE tunnel is on	Zeroization command	IPSec/IKE RSA Public Key:Paired With
IPSec/IKE RSA Public Key	Module Public Key Output	Flash:Plaintext	while IPSec/IKE tunnel is on	Zeroization command	IPSec/IKE RSA Private Key:Paired With
IPSec/IKE Pre-shared Secret	Password/Secret Input encrypted by GCM Password/Secret Input encrypted by AES and HMAC	Flash:Plaintext	while IPSec/IKE v2 tunnel is on	Zeroization command	SKEYSEED:Derived to
SKEYSEED		RAM:Plaintext	while IPSec/IKE v2 tunnel is on	Zeroization command	TLS ECDH Shared Secret:Derived From IPSec/IKE DH Shared Secret:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
IPSec/IKE Encryption Key		RAM:Plaintext	while IPSec/IKE v2 tunnel is on	Zeroization command	IPSec/IKE DH Shared Secret:Derived From IPSec/IKE ECDH Shared Secret:Derived From
IPSec/IKE Authentication Key		RAM:Plaintext	while IPSec/IKE v2 tunnel is on	Zeroization command	IPSec/IKE DH Shared Secret:Derived From IPSec/IKE ECDH Shared Secret:Derived From
SNMPv3 Shared Secret	Password/Secret Input encrypted by GCM Password/Secret Input encrypted by AES and HMAC	Flash:Plaintext	while SNMPv3 tunnel is on	Zeroization command	SNMPv3 Encryption Key:Derive to SNMPv3 Authentication Key:Derive to
SNMPv3 Encryption Key		RAM:Plaintext	while SNMPv3 tunnel is on	Zeroization command	SNMPv3 Shared Secret:Derived From SNMPv3 Authentication Key:Used With
SNMPv3 Authentication Key		RAM:Plaintext	while SNMPv3 tunnel is on	Zeroization command	SNMPv3 Shared Secret:Derived From SNMPv3 Encryption Key:Used With
VLAN Encryption Key	VLAN SSPs Input via TLS-KTS (GCM) VLAN SSPs Input via TLS-KTS (AES and HMAC)	Flash:Plaintext	while VLAN tunnel is on	Zeroization command	VLAN Authentication Key:Used With
VLAN Authentication Key	VLAN SSPs Input via TLS-KTS (GCM) VLAN SSPs	Flash:Plaintext	while VLAN tunnel is on	Zeroization command	VLAN Encryption Key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Input via TLS-KTS (AES and HMAC)				

Table 18: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RSA SigVer (FIPS186-4) (A3316)	Modulus: 4096 bits with SHA2-256	KAT	SW/FW Integrity	Module is in normal state	Module conducts RSA SigVer KAT prior to firmware integrity test

Table 19: Pre-Operational Self-Tests

The module conducts the RSA 4096 modulus with SHA2-256 SigVer KAT prior to the integrity test is performed.

The module also performs the following Cryptographic Algorithm Self-Tests (CASTs), which can be initiated by rebooting the module. All self-tests run without operator intervention. In the event that a self-test fails, the module will enter an error state until the issue is resolved.

Upon self-test failure, the module will go into the SYS_HALT status.

Entropy start-up tests per SP800-90B section 4.2 including Repetition Count Test and Adaptive Proportion Test are performed at device power-on and it will run continuously. Any entropy test failures will cause SYS_HALT.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A3316)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Encrypt	Power up
AES-CBC (A3316)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Decrypt	Power up
AES-CCM (A3316)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Encryption	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CCM (A3316)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Decryption	Power up
AES-GCM (A3316)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Encryption	Power up
AES-GCM (A3316)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Decryption	Power up
Counter DRBG (A3316)	AES-256	Known Answer Test (KAT)	CAST	Module is in normal state	CTR_DRBG Instantiate	Power up
Counter DRBG (A3316)	AES-256	Known Answer Test (KAT)	CAST	Module is in normal state	CTR_DRBG Generate	Power up
Counter DRBG (A3316)	AES-256	Known Answer Test (KAT)	CAST	Module is in normal state	CTR_DRBG Reseed	Power up
ECDSA SigGen (FIPS186-4) (A3316)	P-256 with SHA2-256	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
ECDSA SigVer (FIPS186-4) (A3316)	P-256 with SHA2-256	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
KAS-ECC-SSC Sp800-56Ar3 (A3316)	P-256 with SHA2-256	Known Answer Test (KAT)	CAST	Module is in normal state	KAS-ECC-SSC Primitive Z	Power up
KAS-FFC-SSC Sp800-56Ar3 (A3316)	MODP-2048	Known Answer Test (KAT)	CAST	Module is in normal state	KAS-FFC-SSC Primitive Z	Power up
HMAC-SHA-1 (A3316)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
HMAC-SHA2-256 (A3316)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
HMAC-SHA2-384 (A3316)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
HMAC-SHA2-512 (A3316)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigGen (FIPS186-4) (A3316)	2048 bits	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
RSA SigVer (FIPS186-4) (A3316)	2048 bits	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
SHA-1 (A3316)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
KDF IKEv2 (A3316)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
KDF SNMP (A3316)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
TLS v1.2 KDF RFC7627 (A3316)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
TLS v1.3 KDF (A3316)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
AES-CBC (A3318)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Encryption	Power up
AES-CBC (A3318)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Decryption	Power up
AES-CCM (A3318)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Encryption	Power up
AES-CCM (A3318)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Decryption	Power up
AES-GCM (A3318)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Encryption	Power up
AES-GCM (A3318)	256 bits	Known Answer Test (KAT)	CAST	Module is in normal state	Authenticated Decryption	Power up
HMAC-SHA-1 (A3318)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
HMAC-SHA2-256 (A3318)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-384 (A3318)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
HMAC-SHA2-512 (A3318)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	N/A	Power up
SHA-1 (A3318)	N/A	Known Answer Test (KAT)	CAST	Module is in normal state	SHA-1	Power up
KAS (A3316)	P-256 with SHA2-256	KAS-ECC Pairwise Consistency Test (PCT)	PCT	Module is in normal state	N/A	Before the first operational use
KAS (A3316)	MODP-2048	KAS-FFC Pairwise Consistency Test (PCT)	PCT	Module is in normal state	N/A	Before the first operational use
ECDSA KeyGen (FIPS186-4) (A3316)	P-256 with SHA2-256	ECDSA Pairwise Consistency Test (PCT)	PCT	Module is in normal state	ECDSA	Before the first operational use
RSA KeyGen (FIPS186-4) (A3316)	2048 bits	RSA Pairwise Consistency Test (PCT)	PCT	Module is in normal state	RSA	Before the first operational use
RSA SigVer (FIPS186-4) (A3316)	RSA 4096 bits with SHA2-256	Firmware Load Test	SW/FW Load	Module is in normal state	RSA	while doing the firmware upload test

Table 20: Conditional Self-Tests

The module also performs the following Entropy start-up tests per SP800-90B section 4.2 including Repetition Count Test and Adaptive Proportion Test are performed at device power-on and it will run continuously. Any entropy test failures will cause SYS_HALT.

- Entropy Source Health Tests:
  - SP800-90B Entropy Source Start-up Health Tests:
    - Repetition Count Test (RCT)
    - Adaptive Proportion Test (APT)
  - SP800-90B Entropy Source Continuous Health Tests:
    - Repetition Count Test (RCT)
    - Adaptive Proportion Test (APT)

In addition, the module also supports the firmware load test by using RSA 4096 bits with SHA2-256 (RSA Cert. #A3316) for the new validated firmware to be uploaded into the module. A Firmware Load Test Key was preloaded to the module's binary at the factory and used for firmware load test. In order to load new firmware, the Crypto Officer must authenticate to the module before loading the firmware. This ensures that unauthorized access and use of the module is not performed. The module will load the new update upon reboot. The update attempt will be rejected if the verification fails.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A3316)	KAT	SW/FW Integrity	Recommend every 60 days	Module Reboot

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
AES-CBC (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
AES-CCM (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
AES-CCM (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
AES-GCM (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
AES-GCM (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
Counter DRBG (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
Counter DRBG (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
Counter DRBG (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
ECDSA SigGen (FIPS186-4) (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
ECDSA SigVer (FIPS186-4) (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
KAS-ECC-SSC Sp800-56Ar3 (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
KAS-FFC-SSC Sp800-56Ar3 (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	ReModule Reboot
HMAC-SHA-1 (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
HMAC-SHA2-256 (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-384 (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
HMAC-SHA2-512 (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
RSA SigGen (FIPS186-4) (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
RSA SigVer (FIPS186-4) (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
SHA-1 (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
KDF IKEv2 (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
KDF SNMP (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
TLS v1.2 KDF RFC7627 (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
TLS v1.3 KDF (A3316)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
AES-CBC (A3318)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
AES-CBC (A3318)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
AES-CCM (A3318)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
AES-CCM (A3318)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
AES-GCM (A3318)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
AES-GCM (A3318)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
HMAC-SHA-1 (A3318)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
HMAC-SHA2-256 (A3318)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
HMAC-SHA2-384 (A3318)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
HMAC-SHA2-512 (A3318)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
SHA-1 (A3318)	Known Answer Test (KAT)	CAST	Recommend every 60 days	Module Reboot
KAS (A3316)	KAS-ECC Pairwise Consistency Test (PCT)	PCT	N/A	New KAS ECC Keypair generation

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS (A3316)	KAS-FFC Pairwise Consistency Test (PCT)	PCT	N/A	New KAS FFC Keypair generation
ECDSA KeyGen (FIPS186-4) (A3316)	ECDSA Pairwise Consistency Test (PCT)	PCT	N/A	New ECDSA Keypair generation
RSA KeyGen (FIPS186-4) (A3316)	RSA Pairwise Consistency Test (PCT)	PCT	N/A	New RSA Keypair generation
RSA SigVer (FIPS186-4) (A3316)	Firmware Load Test	SW/FW Load	N/A	N/A

Table 22: Conditional Periodic Information

The module performs on-demand self-tests initiated by the operator, by power cycling to the module. The full suite of self-tests is then executed. The same procedure may be employed by the operator to perform periodic self-tests.

In addition, the Crypto Officer shall perform the periodic test on demand no less than every 90 days to ensure all components are functioning correctly.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	If self-test tests fail, the module is put into an error state	Self-tests failure	Reboot the module	System Halt

Table 23: Error States

If any of the above-mentioned self-tests fail, the module reports the cause of the error and enters the Error state. In the Error State, no cryptographic services are provided, and data output is prohibited. The only method to recover from the error state is to reboot the module and perform the self-tests, including the pre-operational firmware integrity test and the conditional CASTs. The module will only enter into the operational state after successfully passing the pre-operational firmware integrity test and the conditional CASTs.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module operates in the approved mode of operation at all times. The 3e-Local 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. If the external authentication server is employed, please use TLS v1.2 or TLS v1.3 or IPSec/IKEv2 to protect the traffic between the authentication server and the module.
4. Configure the Data VPN tunnel with proper SSPs, such as certificate, private key, trust anchor and key expiration time. Or configure the VLAN encryption services with VLAN tag, authentication key and encryption key.
5. Verify that the module is in the approved mode of operation from the Web GUI.
After configuration of the above items, reboot the device and the device will come back in full approved mode of operation.

Security Rules:
The module meets all the Level 2 requirements for FIPS 140-3. Follow the secure operations provided below to place the module in the approved mode. Operating this module without maintaining the following settings will remove the module from the approved mode of operation. The module runs firmware version 1.0. This is the only allowable firmware image (cn9130-cf-fips.ipsec.6.0.0.00.6.bin) for this current approved mode of operation. The 3e-Local shall load the CMVP FIPS 140-3 validated firmware only to maintain validation.

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

1. The 3e-Local shall not share any SSPs used by the module with any other operator or entity.
2. The 3e-Local 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-Local shall change the default password (default username: CryptoOfficer; default password: CryptoFIPS) when configuring the module for the first time. Please note that the module firmware enforces the password change upon the 3e-Local first log in.
4. The 3e-Local shall login to make sure CSPs and keys are configured and applied in the module.

11.2 Administrator Guidance

No specific Administrator guidance.

11.3 Non-Administrator Guidance

No specific non-Administrator guidance.

11.6 End of Life

Crypto Officer (3e-Local Role and 3e-CyrptoOfficer role) should follow the steps below for the secure destruction of the module:

Note: This process will cause the module to no longer function after it has wiped all configurations and keys.

1. Access the module via HTTPS over TLS v1.2 or TLS v1.3
2. Authenticate to the module as the CO by using the proper credentials
3. Execute zeroization service: “Factory Default”

a. Confirm command

4. Module will begin zeroization process and wipe all security parameters and configurations

12 Mitigation of Other Attacks

Not Applicable as the module does not claim mitigation of other attacks.