FIPS 140-2
Non-Proprietary Security Policy
Level 2 Validation

3e-520
Secure Access Point Cryptographic Module

Hardware Version 1.0
Firmware Version 5.1

Security Policy
Version 2.14

October 3, 2022

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

1.1. Purpose

This document describes the non-proprietary cryptographic module security policy for the *3e-520 Secure Access Point Cryptographic Module (*hereafter referred to as module*)* with Hardware Version: 1.0 and Firmware Version: 5.1 from Ultra. This cryptographic module is used in all Ultra's WiFiProtect series wireless products. This policy was created to satisfy the requirements of FIPS 140-2 Level 2. The cryptographic module security policy consists of a specification of the security rules, under which the cryptographic module shall operate, including the security rules derived from the requirements of the standard. Please refer to FIPS 140-2 Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules* available on the NIST website at https://csrc.nist.gov/Projects/cryptographic-module-validation-program/publications.

1.2. Definition

The *3e-520 Secure Access Point Cryptographic Module* consists of electronic hardware, embedded firmware and an enclosure. For purposes of FIPS 140-2, the module is considered to be a multi-chip embedded module. 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).

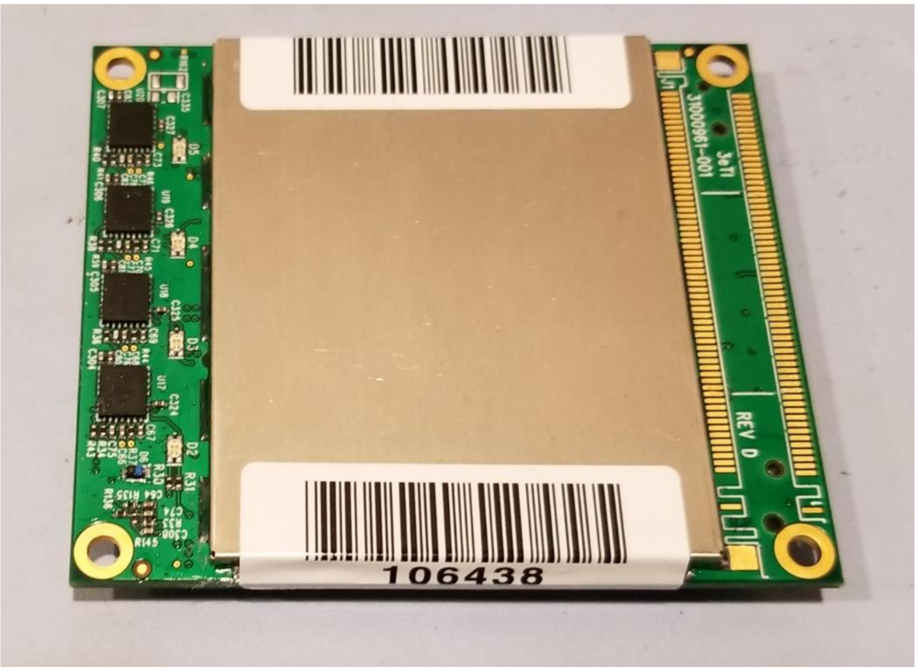

Figure 1 – 3e-520 Secure Access Point Cryptographic Module

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. The table below lists the security level of this module.

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

1.3. *Ports and Interfaces*

The module provides Ethernet port pins, PCI connectors for wireless radios, general purpose IO pins (GPIO) for LEDs and serial communication and power input as shown in the figure below:

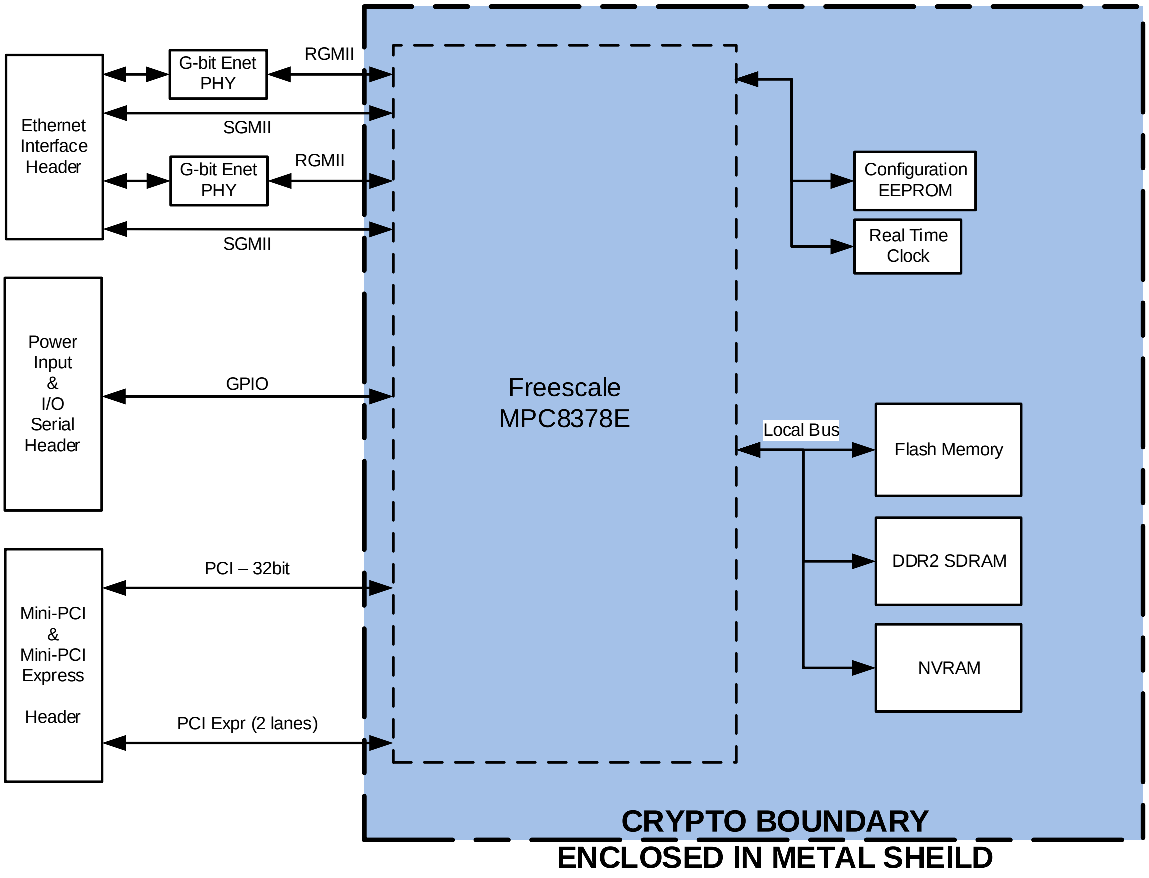

Figure 2 – Module High Level Block Diagram

The ports are defined below:

a. Status output: Ethernet port pins and LED (GPIO) pins
b. Data output: Ethernet port pins, serial port pins and PCI pins
c. Data input: Ethernet port pins, serial port pins and PCI pins
d. Control input: Ethernet port pins and PCI pins
e. Power input: GPIO pins

1.4. *Scope*

This document covers the secure operation of the *3e-520 Secure Access Point Cryptographic Module*, including the initialization, roles and responsibilities of operating the module in a secure, FIPS-compliant manner, and a description of the Security Relevant Data Items (SRDIs).

2. Roles, Services, and Authentication

The module supports four separate roles. The set of services available to each role is defined in this section. The module authenticates an operator's role by verifying his/her password or possession of a shared secret.

2.1. 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 (Crypto Officer) authenticates to the module using a username and password. The 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 3e-520 series Remote A&A settings.

3e-Administrator Role: This role performs the module's general 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.

User Role: The purpose of the user role is to describe other devices as they interact with this Cryptographic Module, including:

- Other Access Points (connecting in Bridge mode)
- WLAN Client
- Security Server
- IPsec Peer

The User Role has access to the following services:

For User Role (WLAN client)

- ➢ Apply Wireless Access Point Security on Data Packet
  - ▪ 802.11i AES-CCM

For User Role (AP)

- ➢ Apply Wireless Bridge Encryption on Data Packet
  - ▪ AES
  - ▪ AES_CCM
- ➢ Communicate with Security Server for Authentication and Key Setting
  - ▪ AES KeyWrap

- For User Role (IPsec Peer)
  - ➢ Apply IPsec ESP encryption on Data Packet
    - ▪ AES_GCM

Administrative users such as 3e-CryptoOfficer (of 3e-local group) and 3e-Administrator use the HTTPS interface to manage the module.

SNMP v3 interface is also supported by the module. It supports both SNMP GETs and SETs. However, the GETs and SETs are applicable to non-security related parameters only. CSPs, Keys, password and other security related configuration parameters are not accessible through SNMP. Neither GETs nor SETs are supported for those parameters.

The following table outlines the security-relevant cryptographic functionalities that are provided by the “operator” roles (3e-local, 3e-CryptoOfficer and 3e-Administrator).

Table 2 – Operator Role Functionalities

Services	Features	Operator Roles												CSP Access (CSP ID table 6)
		3e-local & 3e-CryptoOfficer						3e-Administrator						
		Show[1]	Set[2]	Add[3]	Delete[4]	Zeroize[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Zeroize[11]	Default Reset	
System Configuration														
General		**X**	**X**					**X**	**X**					None
Noisy Channel Control		**X**	**X**					**X**	**X**					None
WAN		**X**	**X**					**X**	**X**					None
LAN		**X**	**X**					**X**	**X**					None
Bridge		**X**	**X**					**X**	**X**					None
Ethernet VLAN		**X**	**X**											None
MAC Address Filtering		**X**	**X**	**X**	**X**			**X**						None
Certificate Store		**X**	**X**	**X**	**X**									16,20,21
Radio														
WLAN Mode		X	X					X	X					None
PHY Setting		X	X					X	X					None
AP General		X	X					X	X					None
Wireless VLAN Mapping		X	X					X	X					None
AP Security	AES (128-/192-256-bit) 802.11i (AES-CCM)	X	X											7,13,14,15
AP Wireless Clients		X						X						
IPsec Tunnel														
Profiles		X	X	X	X			X		X	X			None
Status		X						X						None
Services Settings														
DHCP Server		X	X					X	X					None
SNMP Agent		X	X					X	X					3,4
Serial Port		X	X					X	X					None
Serial Communication		X	X					X	X					None
Web Server		X	X											16
Remote Administration		X	X					X	X					None

Services	Features	Operator Roles												CSP Access (CSP ID table 6)
		3e-local & 3e-CryptoOfficer						3e-Administrator						
		Show[1]	Set[2]	Add[3]	Delete[4]	Zeroize[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Zeroize[11]	Default Reset	
Admin User Management														
List all Users		X												None
Add New User		X	X	X										1
User Login Policy		X	X											None
Remote A&A Setup		X	X											None
Two-Factor Auth		X	X											None
Monitoring/Reports														
System Status		X						X						None
Bridge Status		X						X						None
Bridging Site Map		X						X						None
Adjacent AP List		X						X						None
DHCP Client List		X			X			X						None
Logs														
System Log		X						X						None
Web Access Log		X						X						None
Auditing														
Audit Configuration		X	X											None
Audit Log		X	X					X	X					None
System Administration														
Email Notification Conf		X	X											None
Radio Tx Control		X	X											None
System Upgrade		X	X											2,5
Default Configuration		X	X				X							None
Remote Logging		X	X					X	X					None
Reboot		X	X					X	X					None
On Demand Self-test		X	X											None
Periodic Self-test		X	X											None
Password	Change password for Crypto Officer		X	X	X		X							1
	Change password for Administrator		X	X	X		X		X					
	Change password policy for Crypto Officer		X				X							
	Change password policy for Administrator		X				X							

Services	Features	Operator Roles												CSP Access (CSP ID table 6)
		3e-local & 3e-CryptoOfficer						3e-Administrator						
		Show[1]	Set[2]	Add[3]	Delete[4]	Zeroize[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Zeroize[11]	Default Reset	
Utility		X	X					X	X					
Help		X						X						

[1] *The operator can view this setting.*
[2] *The operator can change this setting.*
[3] *The operator can add a required input.*
[4] *The operator can delete a particular entry.*
[5] *The operator can zeroize these keys.*
[6] *The operator can reset this setting to its factory default value.*
[7] *The operator can view this setting.*
[8] *The operator can change this setting.*
[9] *The operator can add a required input.*
[10] *The operator can delete a particular entry.*
[11] *The operator can zeroize these keys.*

The following table outlines the security-relevant cryptographic functionalities that are provided to the User Role:

Table 3 – User Role Functionalities

Services	Features	User Role					CSP Access (table 6 CSP ID)	
		Show	Apply	Add	Delete	Zeroize	Default Reset	
Wireless Access Point								
Encryption	AES (128/192/256-bit) 802.11i (AES-CCM)		X X			X X		9, 10, 11, 12, 13, 14
Wireless Bridge								
Encryption	AES (128/192/256-bit) AES_CCM(128 bit)		X X			X X		17
Wireless Client								
Encryption	802.11i (AES-CCM)		X			X		9,10,11,12,13,14
Security Server								
Encryption	AES Key wrap		X			X		16
IPsec								
Encryption	AES, AES-CCM, AES-GCM (128,192,256)		X			X		6,7,8,27,29,30,31,32,33,34,35,36
TLS								
Encryption	AES (128,192,256)		X			X		18,19,20,21,22,23,24,25,26

2.2. *Authentication Mechanisms and Strength*

The module employs identity-based and role-based authentication to control access to the module. The Crypto Officer (of 3e-local, 3e-CryptoOfficer and 3e-Administrator) and User use the following authentication methods to access the module:

Table 4 – Authentication versus Roles

Role	Type of Authentication	Authentication Data
Crypto Officer		
3e-local	ID-based	Userid and password
3e-CryptoOfficer	ID-based	Userid and password
3e-Administrator	ID-based	Userid and password
User		
Wireless client	Role-based, 802.11i authentication between wireless client and Device with X.509 certificate or PMK	X.509 certificate or PMK, identifiable with MAC address
AP	Role-based, static key	static key, identifiable with MAC address
IPsec Peer	ID-based, IPsec IKEv2 authentication	X.509 certificate or PSK Identifiable with IP address

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

Table 5 – Strength of Authentication

Authentication Mechanism	Strength of Mechanism
Password and UserID	8-32 characters => 94^8 = 6.096E15
Digital certificates (for 802.11 client using EAP-TLS or IPsec peer)	Private keys in certificates => 112 bits security => 2^112 = 5.19E33
PMK (for 802.11 client)	256 bits => 2^256 = 1.157E77
PSK (for IPsec peer)	256 bits => 2^256 = 1.157E77
Bridging static AES key (128/196/256) bits	128 bits => 2^128 = 3.40E38

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 while WLAN is 400Mbps. 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 minutes 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.

3. Operation Guidance and Secure Operation

The module has only one mode of operation, the FIPS mode. The factory default of the device is set with no security setting and the radio turned off. The device requires the 3e-local operator to change the default password when configuring the device for the first time.

3.1. Operator Guidance

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

1. Every operator (3e-CryptoOfficer or 3e-Administrator) was assigned a distinguished user-ID to access to the module. No operator shall violate trust by sharing his/her password associated with the user-id with any other operator or entity.
2. The 3e-CryptoOfficer shall not share any key, or SRDI used by the module with any other operator or entity.
3. The 3e-CryptoOfficer shall not share any MAC address filtering information used by the module with any other operator or entity.
4. The operators shall explicitly logoff by closing all secure browser sessions established with the module.
5. The 3e-CryptoOfficer is responsible for inspecting the tamper evident seals. Other signs of tamper include wrinkles, tears and marks on or around the label.
6. The *3e-CryptoOfficer* shall load the FIPS validated firmware only.

3.2. Secure Operation

1. The 3e-CryptOfficer shall login to make sure encryption is applied in the device.
2. The 3e-CryptoOfficer shall configure the device to use “IETF” as RADIUS type for wireless clients authentication using 802.1X. RADIUS type of “3eTI” shall NOT be used.
3. If IPsec tunnel is configured, the SA rekey policy based on packet counter shall be configured between the allowed values: 192 - 2097151*K.*
4. 3e-CryptoOfficer shall configure and setup the IPsec tunnel for 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.

3.3. Physical Security Tamper Evidence

The module is a multi-chip embedded cryptographic module and conforms to Level 2 requirements for physical security. All components are production-grade materials with standard passivation. The module's physical security 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.

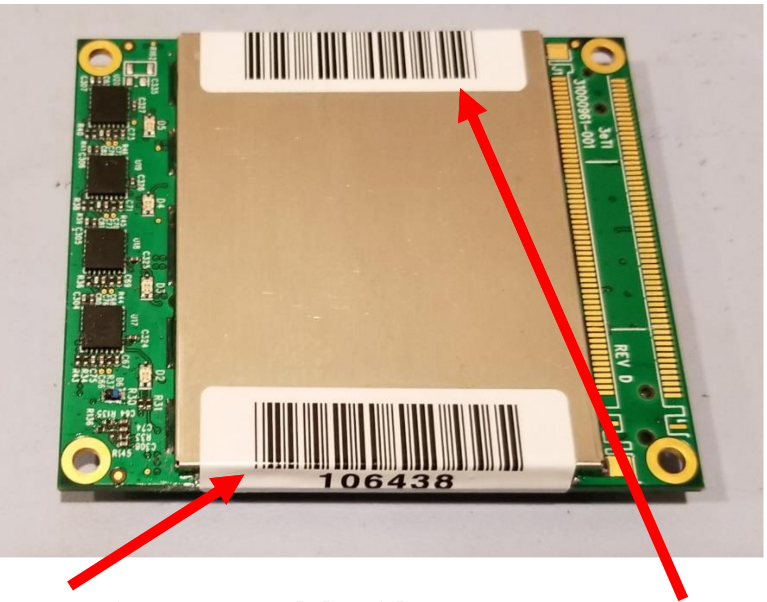

Figure 3 – Module with TELs

<u>Checking for Tamper Evidence</u>

Tamper evidence labels 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.

4. Security Relevant Data Items

This section specifies the module's Security Relevant Data Items (SRDIs) as well as the module-enforced access control policy.

4.1. 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.

Table 6 – FIPS Algorithms

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
Ultra MPC8378E Cryptographic Core					
A1701	AES	FIPS 197, SP800-38A	CBC, ECB, CCM, GCM	128, 192, 256	Data Encryption/Decryption
A1701	KTS by using AES-CCM	SP800-38F	KTS (AES Cert. #A1701; key establishment methodology provides between 128 and 256 bits of encryption strength)	128, 192, 256	Key Wrapping/Unwrapping
A1701	HMAC	FIPS 198-1, FIPS 180-4	SHA-1, SHA2-224, SHA2-256	128	Keyed Hash
			SHA2-384,	192	
			SHA2-512	256	
A1701	Secure Hashing	FIPS 180-4	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512		Secure Hashing
Ultra OpenSSL Algorithm Implementation					

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
A1702	AES	FIPS 197, SP800-38A	ECB, CBC	128, 192, 256	Data Encryption/Decryption
A1702	KTS by using AES and HMAC	SP800-38F	KTS (AES Cert. #A1702 and HMAC Cert. #A1702; key establishment methodology provides between 128 and 256 bits of encryption strength)	AES-128, AES-196, AES-256	Key Wrapping/Unwrapping
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	FIPS 186-4	KeyGen, KeyVer, SigGen, SigVer	P-256, P-384, P-521	Digital Signature Generation and Verification. Key Generation and Verification
A1702	HMAC	FIPS 198-1, FIPS 180-4, FIPS 202	SHA-1, SHA2-224, SHA2-256, SHA3-224, SHA3-256	128	Keyed Hash ** SHA3 Tested by CAVP but not used by module*
			SHA2-384, SHA3-384	192	
			SHA2-512, SHA3-512	256	
A1702	Secure Hashing	FIPS 180-4, FIPS 202	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512,		Secure Hashing **SHA3 tested by CAVP but not used by module*

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
			SHA3-224, SHA3-256, SHA3-384, SHA3-512		
A1702	RSA	FIPS 186-4	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	KBKDF	SP800-108	KDF Mode: Counter MAC Mode: HMAC-SHA2-256		Key Derivation used by IEEE 802.11
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	SP800-56Arev3; SP800-135rev1	KAS (ECC): ephemeralUnified:	KAS (ECC): P-256, P-384 and P-521 with IKEv2 KDF	Key Agreement Scheme per SP800-56Arev3 with key derivation

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
	Cert. #A1702, CVL Cert. #A1702)		KAS Role: initiator, responder KAS (FFC): dhEphem: KAS Role: initiator, responder	(SP800-135rev1); KAS (FFC): ffdhe2048, MODP-2048 with TLSv1.2 and IKEv2 KDF (SP800-135rev1)	function (SP800-135rev1) Note: The module's KAS (ECC/FFC) implementation is FIPS140-2 IG D.8 Scenario X1 (path 2) compliant
N/A	CKG (Vendor affirmed)	SP800-133rev2			Cryptographic Key Generation as per section 6 in SP800-133rev2
Ultra Linux Kernel Cryptographic Library					
A2152	Secure Hashing	FIPS 180-4	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.

4.2. 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 bits of encryption strength)

5. Self-tests

The module performs the following power-up and conditional self-tests. In addition to performing the power-up tests when powered up, the module also permits the operators to initiate the tests on demand periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly.

Upon failure of a power-up or conditional self-test, the module would enter into the error state (halts the operation). POST (Power on Self Tests) is performed on each boot. A command to reboot the device is considered on-demand self-test. Both “3e-CryptoOfficer” and “3e-Administrator” roles can send reboot command from web GUI.

5.1. Power-on Self-tests

Ultra OpenSSL Power-on self-tests:

• 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 (using ECDSA PWCT Sign and Verify)	
• RSA sign/verify KATs (separate KAT for signing; separate KAT for verification)	
• SP800-90A CTR_DRBG (DRBG health tests per SP800-90A Section 11.3)	KAT
• SP800-135 TLS 1.2 KDF	KAT
• SP800-135 SNMPv3 KDF	KAT
• SP800-135 IKEv2 KDF	KAT
• KAS-ECC-SSC Primitive Z	KAT
• KAS-FFC-SSC Primitive Z	KAT
• KBKDF (SP800-108)	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 CCM 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 3.6 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, firmware won’t boot. Firmware integrity is also performed at POST (Power On Self-Test) 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.

In addition to performing the power-up tests when powered up, the Crypto Officer shall perform the periodic test on demand no more than 30 days (i.e., once/month) to ensure all components are functioning correctly.

5.2. 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)

6. Cryptographic Keys and SRDIs

The module contains the following security relevant data items:

Table 7 – SRDIs

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	Plaintext in flash	Zeroized when reset to factory settings.	Used to authenticate CO and User role operators
2	Firmware verification key	ECDSA P-256 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 key	HMAC key (ASCII string) 20 bytes	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	Zeroized when reset to factory settings.	Used by SNMP KDF
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						
CSP ID	**Key/CSP**	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
6	DRBG CTR V	32-byte value	Internally derived by OpenSSL DRBG after a 256 bit seed and 128 bit nonce are read from /dev/random	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	Internally derived by OpenSSL DRBG after a 256 bit seed and 128 bit nonce are read from /dev/random	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 802.11 Protocol Keys/CSPs						
CSP ID	**Key/CSP**	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
9	PMK	32 bytes 802.11i pairwise master key	If 802.11i PSK, it's input directly as a Hex string. Input encrypted using the TLS session key. If 802.11i EAP-TLS, then not input, instead derived (TLS master secret resulting from successful User EAP-TLS authentication)	Not output	If 802.11i PSK, then plaintext in flash For both 802.11i PSK and EAP-TLS, plaintext in RAM	Zeroized when wireless user disconnect or at PMK expiration. If 802.11i PSK, zeroized when reset to factory settings.	802.11i PMK
10	KCK	HMAC key (128 bits from PTK)	Not input (derived from PMK)	Not output	Plaintext in RAM	When 802.11i session ends.	802.11i KCK
11	KEK	AES-CCM (e/d; 128 bits)	Not input (derived from PMK)	Not output	Plaintext in RAM	When 802.11i session ends.	802.11i KEK
12	PTK	AES-CCM (e/d; 128 bits)	Not input (derived from PMK)	Not output	Plaintext in RAM	When 802.11i session ends.	802.11i TK
13	PTK (copy in driver)	AES-CCM (e/d; 128 bits)	Not input (derived from PMK)	Not output	Plaintext in RAM	When 802.11i session ends.	802.11i TK
14	GTK	AES-CCM (e/d; 128 bits)	Not input (derived from PMK & 802.11i)	Output encrypted (using KEK)	Plaintext in RAM	Zeroized when local antennae Approved encrypting mode either reconfigured or changed from IEEE 802.11i mode to any other local antennae Approved encrypting mode (including from 802.11i PSK to 802.11i EAP-TLS, and 802.11i EAP-TLS to 802.11i PSK). When re-key period expires.	802.11i GTK

	Ultra Security Server Keys/CSPs						
CSP ID	**Key/CSP**	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
15	Security Server Password	HMAC key (ASCII string) 20 bytes	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	Zeroized at factory default reset.	Authenticate module to Security Server in support of 802.11i EAP-TLS authentication
16	Security Server Key Wrap Key	AES-CBC (256 bits) with HMAC	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	Zeroized at factory default reset.	Wrap the PMK sent from Security Server
	Ultra Bridging Protocol Keys/CSPs						
CSP ID	**Key/CSP**	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
17	Bridging static key	AES ECB (e/d ; 128,192, 256 bits) AES-CCM (128 bits)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	Zeroized at factory default reset.	Used to encrypt bridged traffic between two modules
	RFC 2818 HTTPS Keys/CSPs						
	Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
18	RSA private key	RSA (2048 bits) (key wrapping; key establishment methodology provides 112 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 the web server certificate is deleted from certificate store and when firmware is upgraded.	Used to support CO and User HTTPS interfaces.
19	RSA public key	RSA (2048 bits)	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.
20	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.
21	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.
22	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.
23	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.
24	TLS master secret	48 bytes	Not input, derived from	Not output	Plaintext in RAM	Zeroized when session terminated.	Used to protect HTTPS session.

			TLS pre-master secret				
25	TLS session key for encryption	AES (128/192/256 bits)	Not input, derived from TLS master secret	Not output	Plaintext in RAM	Zeroized when session terminated.	Used to protect HTTPS session.
26	TLS session key for message authentication	HMAC (128/192/256 bits)	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.
	IPsec Protocol Keys/CSPs						
	Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
27	DH Private Key	224 bits	Generated	None	Plaintext in RAM	Zeroized when no longer used.	IKE v2 SA setup
28	DH Public Key	2048 bits	Generated	Output to peer	Plaintext in RAM	Zeroized when no longer used.	IKE v2 SA setup
29	ECCDH Private Key	P-256, P-384, P-521	Generated	None	Plaintext in RAM	Zeroized when no longer used.	IKE v2 SA setup
30	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
31	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
32	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
33	IPSec IKE SA authentication certificate private key	RSA (2048,3072) ECDSA (P-256,P-384,P-521)	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
34	IPSec IKE SA authentication 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
35	IPSec IKE SA session key	AES (128/192/256 bits)	Derived from DH/ECCDH key exchange	Not output	Plaintext in RAM	Zeroized when no longer used.	Encrypt and authenticate IKE v2 SA messages
36	IPSec ESP Data encryption key	AES, AES_CCM, AES_GCM (128,192,256 bits)	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

Besides the cryptographic keys and CSPs listed in Table 7 above, the following is a table of cryptographic keys and CSPs that are unique to the module when it is operating in wireless Client mode:

Table 8 – SRDIs in Client Mode

Non-Protocol Keys/CSPs							
CSP ID	**Key/CSP**	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
1	Certificate Authority (CA) public key certificate	RSA/ECDSA CA certificate	Input encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when reset to factory settings or delete from certificate store.	Used to verify peer public key
2	Client public key certificate	RSA/ECDSA certificate	Input encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when reset to factory default or deleted from certificate store.	Used for EAP-TLS authentication between client and RADIUS server
3	Client private key	RSA private key (2048/3072)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with “system config AES key”	Zeroized when reset to factory settings.	Used for EAP-TLS authentication between client and RADIUS server

7. Design Assurance

All source code and design documentation for this module are 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.

The cryptographic module (CM) 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 verified customer, the part number together with shipping instructions is sent to manufacture. The manufacture builds and pack per instruction and generates a Traveler for each device which includes hardware and firmware versions per unit. Then manufacture checks the label to ensure the unit matches with 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.