3e Technologies International, Inc.
FIPS 140-2
Non-Proprietary Security Policy
Level 2 Validation

3e-520
Secure Access Point Cryptographic Module

HW Versions 1.0
FW Versions 5.0

Security Policy
Version 1.5

June 2013

Glossary of terms

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
PRNG	Pseudo Random Number Generator
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 3e Technologies International's wireless universal products, the *3e-520 Secure Access Point Cryptographic Module* (Hardware Versions: HW V1.0, Firmware Versions: 5.0). This Cryptographic Module is used in all 3eTI 500 series wireless products. This policy was created to satisfy the requirements of FIPS 140-2 Level 2. It defines 3eTI's security policy and explains how the *3e-520 Secure Access Point Cryptographic Module* meets the FIPS 140-2 security requirements.

The figure below shows the *3e-520 Secure Access Point Cryptographic Module*.

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

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 http://csrc.nist.gov/groups/STM/index.html.

1.2. Definition

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

Access Point Cryptographic Module is enclosed in a tamper-resistant opaque metal enclosure, protected by tamper-evident tape intended to provide physical security. This device always runs in FIPS mode. The components attached to the underside of the PCB and the components (RTC, reset delay chip, logic gates, and resistors, underside of chip pads, impedance beads and capacitors) which reside outside of the protective "can" of the module are excluded from FIPS requirements. The table below lists the security level of this module.

Table 1 – Module Security Level

Security Requirements	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2
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:

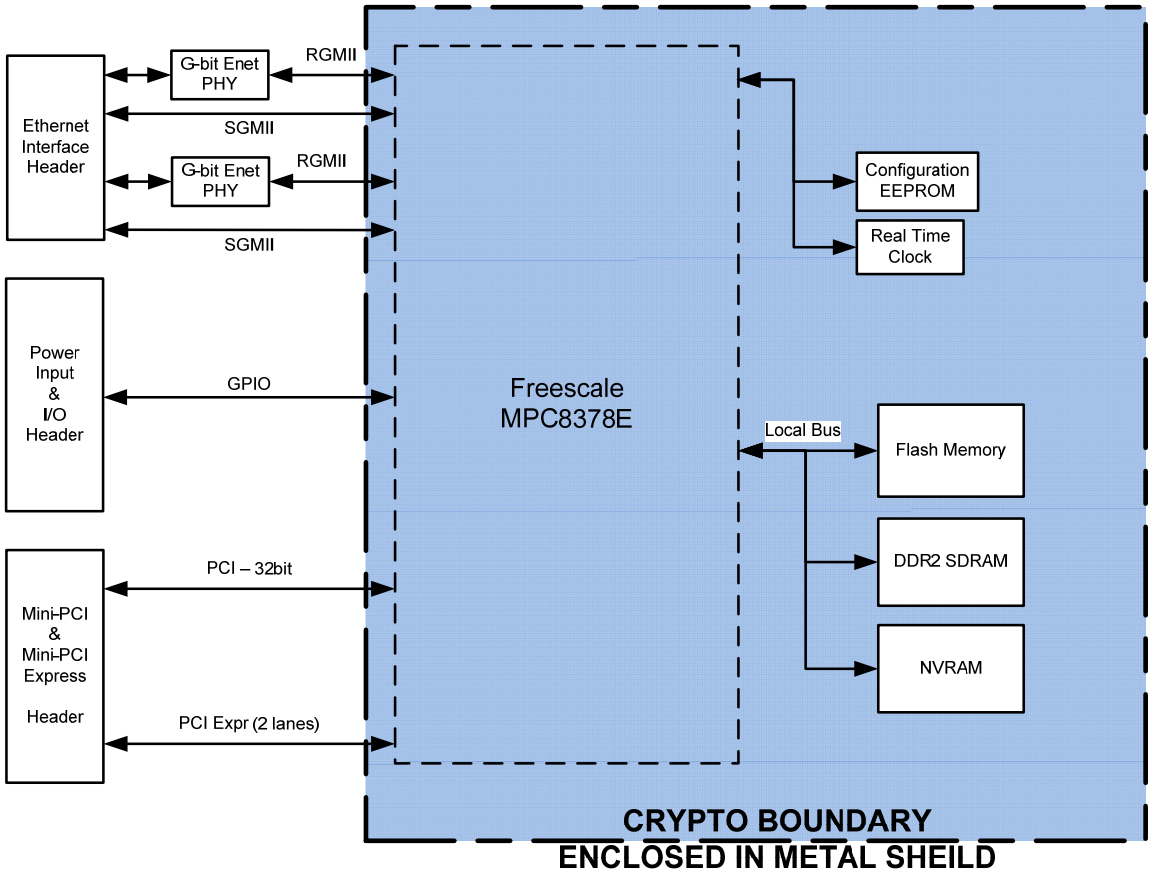


Figure 2 – 3e-520 Wireless Data Point Cryptographic Module High Level Block Diagram

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

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 product in a secure, FIPS-compliant manner, and a description of the Security Relevant Data Items (SRDIs).

2. Roles, Services, and Authentication

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

2.1.1. Roles & Services

The product supports the following authorized roles for operators:

Crypto Officer Role: The Crypto officer (CO) role performs all security functions provided by the product. 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 Crypto officer is also responsible for managing the Administrator users. The Crypto Officer authenticates to the product using a username and password. The Crypto Officer is responsible for managing (creating, deleting) Administrator users.

Administrator Role: This role performs general product configuration. No CO security functions are available to the Administrator. The Administrator can also reboot the product if deemed necessary. The Administrator authenticates to the product 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

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
  - Triple-DES
  - AES
  - AES_CCM
- Communicate with Security Server for Authentication and Key Setting
  - AES KeyWrap

The following table outlines the security-relevant cryptographic functionalities that are provided by the "operator" roles (Crypto Officer and Administrator):

Table 2 – Operator Role Functionalities

Categories	Features	Operator Roles											
		CryptoOfficer						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													
Wireless Access Point													
• Security	AES (128-/192-256-bit) 802.11i (AES-CCM)	X X X X X	X X X X X			 X X X	X X X X X						X X X X X
Wireless Bridge													
• Encryption	Triple-DES AES (128-/192/256-bit) AES_CCM (128 bit)	X X X	X X X		 X X	 X X	X X X						X X X
Monitoring /													

Categories	Features	Operator Roles											
		CryptoOfficer						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
Reports													
• System Status	Security Mode	X						X					
	Current Encryption Mode	X						X					
	Bridging encryption mode	X						X					
	Network Access Logs	X						X					
System Administration													
• Factory Defaults		X	X										
• Reboot (perform self-test)		X	X					X	X				
• Operating Mode	Select wireless operating mode among AP, bridge, AP&bridge, client modes	X	X				X	X					X
• Firmware Upgrade	Upgrade firmware and bootloader if bootloader is included in upgrade package.	X	X										
• Password	Change password for Crypto Officer		X				X						
	Change password for Administrator		X	X	X		X		X				
	Change password policy for Crypto Officer		X				X						
	Change password policy for Administrator		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

Categories	Features	User Role					
		Show	Apply	Add	Delete	Zeroize	Default Reset
Wireless Access Point							
• Encryption	AES (128-/192-256-bit) 802.11i (AES-CCM)		X X X X X			X X X X	
Wireless Bridge							
• Encryption	Triple-DES AES (128-/192-256-bit) AES_CCM(128 bit)		X X X			X X X	
Wireless Client							
• Encryption	802.11i (AES-CCM)		X			X	
Security Server							
• Encryption	AES Key wrap		X			X	

2.1.2. Authentication Mechanisms and Strength

The 520 employs identity-based authentication to control access to the 520 as follows: when the Crypto Officer or Administrator logs in, he/she is required to enter a userid and password. The password is used to authenticate the identity of the operator. A role is implicitly associated with each userid and tracked by the 520. For the User role (client workstation or wireless bridge), the user is uniquely identified by its MAC address while the RADIUS user is uniquely identified by its IP address. The Crypto-Officer is responsible for properly configuring the module's MAC access list and RADIUS server IP address.
The following table summarizes the roles and the type of authentication supported for each role:

Table 4 – Authentication versus Roles

Role	Type of Authentication	Authentication Data
Crypto Officer	ID-based	Userid and password
Administrator	ID-based	Userid and password
User Wireless client	802.11i authentication between wireless client and Device,	The possession of PTK, identifiable with MAC address
AP	Static key	The possession of the static key, identifiable with MAC address
Security Server (RADIUS)	802.1x EAP protocol between security server and Device.	Key Wrapper key and authentication key, 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
Userid and password	Minimum 8 characters => 94^8 = 6.096E15
PSK	128 bits => 2^128 = 3.40E38
Digital certificates	Private keys in certificates => 128 bits => 2^128 = 3.40E38
Shared secret	128 bits => 2^128 = 3.40E38
Bridging static key	128 bits => 2^128 = 3.40E38

Administrative users such as Crypto-Officer and Administrator uses the HTTPS interface to manage the module with underneath TLS protocol's cipher set to AES or 3DES.

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 or SETs are supported for those parameters.

3. Secure Operation and Security Rules

By factory default, the device is put in FIPS mode with NO security setting, and the radio is turned off.

In order to operate the product securely, each operator shall be aware of the security rules enforced by the module and shall adhere to the physical security rules and secure operation rules detailed in this section.

3.1. Security Rules

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

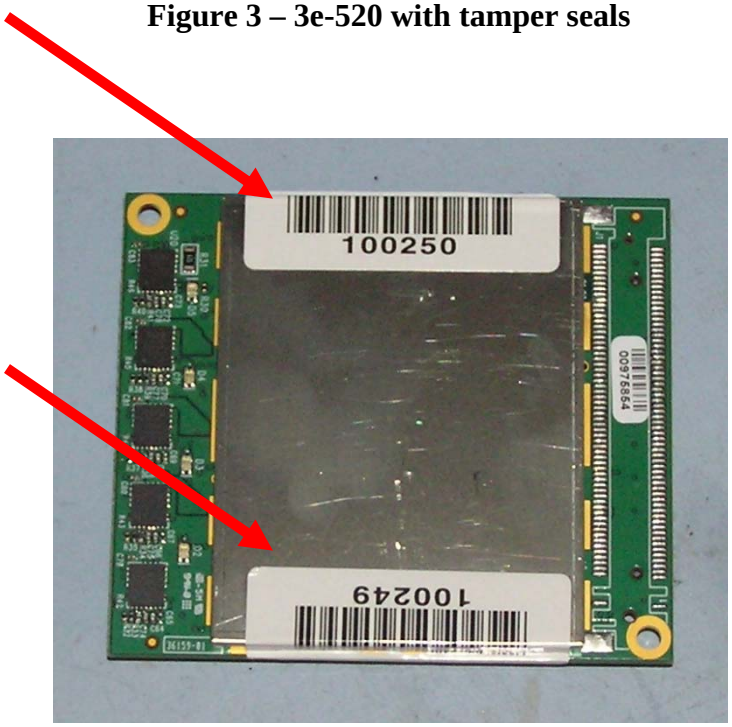
1. Every operator (Crypto Officer or Administrator) has a user-id on the product. No operator shall violate trust by sharing his/her password associated with the user-id with any other operator or entity.
2. The Crypto Officer shall not share any key, or SRDI used by the product with any other operator or entity.
3. The Crypto Officer shall not share any MAC address filtering information used by the product with any other operator or entity.
4. The operators shall explicitly logoff by closing all secure browser sessions established with the product.
5. The Crypto officer is responsible for inspecting the tamper evident seals. Other signs of tamper include wrinkles, tears and marks on or around the label.
6. The Crypto Officer shall change the default password when configuring the product for the first time. The default password shall not be used.
7. The Crypto Officer shall login to make sure encryption is applied in the device.

3.2. Physical Security Tamper Evidence

The physical security provided is intended to meet FIPS 140-2 Level 2 physical security (i.e. tamper evidence). The tamper evidence tape is applied at the factory. Crypto Officer should check the integrity of the tape. 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 3eTI.

The picture below shows the physical interface side of 3e-520 enclosure with tamper-evident seals.

Figure 3 – 3e-520 with tamper seals



4. Security Relevant Data Items

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

4.1. Cryptographic Algorithms

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

3e Technologies International Inc. 3eTI OpenSSL Algorithm Implementation 1.0.1-a

Triple-DES:	#1327
AES:	#2060
SHS:	#1801
RSA:	#1072
HMAC:	#1253
ECDSA verify with P256 curve	#303
RNG:	#1076
Component Test (TLS 1.0/1.1/1.2 with SHA-256/SHA-384)	#22

3e Technologies International Inc. 3e-520 Accelerated Crypto Core 1.0

Triple-DES:	#1329
AES (CCM, CMAC)	#2078
AES (GCM)	#2105
SHS:	#1807
HMAC:	#1259

The product also supports the following **non-Approved but FIPS allowed** cryptographic algorithms:

- RSA (key wrapping, key establishment methodology provides 112 bits of encryption strength)
- MD5 hashing in HTTPS over TLS
- AES (#2060 key wrapping; key establishment methodology provides between 128 and 256 bits of encryption strength)
- Non-Approved RNG for Approved RNG seed and seed key generation.

The product also supports the following **non-Approved FIPS** cryptographic algorithms:

- DES CBC (non-approved) (used in SNMP v3)
- AES CFB (non-compliant) (used in SNMP v3)

SNMP v3 KDF has not been tested and is non-compliant. SNMP v3 is allowed in FIPS mode, but does not protect sensitive information. DES CBC and AES CFB are the two

non-compliant algorithms used by SNMPv3 to obfuscate the PDU packets between it and the external SNMP manager.

4.2 Self-tests

POST (Power on Self Tests) is performed on each boot. A command to reboot the device is considered on-demand self test. Both "Crypto Officer" and "Administrator" roles can send reboot command from web GUI.

4.2.1 Power-on Self-tests

3eTI OpenSSL Power-on self-tests:

- AES ECB CBC 128/192/256 bit – encrypt/decrypt KAT
- Triple-DES CBC – 2 keys and 3 keys encrypt/decrypt KAT
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-521 KAT
- HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 KAT
- RSA SHA1, SHA224, SHA256, SHA384, SHA512 verify test KAT
- ANSI X9.31 RNG KAT
- TLS 1.0/1.1 and 1.2 KDF with SHA256/SHA384 KAT

FreeScale MPC8378E Crypto Engine Power-on self-tests:

- AES ECB, CBC 128/192/256 - encrypt/decrypt KAT
- Triple-DES ECB, CBC - encrypt/decrypt KAT
- AES_CCM – encrypt/decrypt KAT
- SHA-1, SHA224, SHA256, SHA384, SHA512 KAT
- HMAC SHA-1, SHA224, SHA256, SHA384, SHA512 KAT
- AES-CMAC KAT

Software Integrity Test

- Firmware Integrity Test with ECDSA P256 curve verify
- Bootloader Integrity Test with ECDSA P256 curve verify

After device 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.

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.

4.2.2 Conditional Self-tests

Whenever a firmware package is uploaded through HTTPS over TLS secure channel, the package integrity check is performed before the firmware can be updated. The firmware package is digitally signed with 3eTI ECDSA private key and the crypto module performs ECDSA verify before accepting the firmware.

Whenever a random number is generated (both ANSI X9.31 Approved and non-Approved), a Continuous Random Number Generator test is performed to ensure the random number is not repeating.

4.4 Cryptographic Keys and SRDIs

The module contains the following security relevant data items:

Table 6 - SRDIs

Non-Protocol Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
Operator passwords	ASCII string	Input encrypted (using TLS session key)	Not output	Plaintext	Zeroized when reset to factory settings.	Used to authenticate CO and Admin role operators
Firmware verification key	ECDSA public key	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
SNMP packet authentication keys,	HMAC key (ASCII string)	Input encrypted (using TLS	Not output	Ciphertext in flash, encrypted	Zeroized when reset to factory	Use for SNMP message

username		session key)		with "system config AES key"	settings.	authentication
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
RNG Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
FIPS ANSI X9.31RNG Seed Key	16-byte value	512 bytes from system interrupt numbers hashed by HMAC-SHA256	Not output	Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS PRNG after it is used.	Used to initialize FIPS RNG
RNG Seed	16-byte value	512 bytes from system interrupt numbers hashed by HMAC-SHA256		Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS PRNG after it is used.	Used as seed for FIPS RNG.
3eTI 802.11 Protocol Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
PMK	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
KCK	HMAC key (128 bits from PTK)	Not input (derived from PTK)	Not output	Plaintext in RAM	When 802.11i session ends.	802.11i KCK
KEK	AES ECB(e/d; 128)	Not input (derived from PTK)	Not output	Plaintext in RAM	When 802.11i session ends.	802.11i KEK
PTK	AES CCM	Not input	Not output	Plaintext in	When 802.11i	802.11i TK

	(e/d; 128)	(derived from PTK)		RAM	session ends.	
PTK (copy in driver)	AES CCM (e/d; 128)	Not input (derived from PTK)	Not output	Plaintext in RAM	When 802.11i session ends.	802.11i TK
GTK	AES CCM (e/d; 128)	Not input (derived from GMK)	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
3eTI Security Server Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
Security Server password	HMAC key (ASCII string)	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
Backend password	HMAC key (ASCII string)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	Zeroized at factory default reset	Authenticate messages between module and security server in support of 802.11i EAP-TLS
Backend key	AES keywrap key (d;128)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	Zeroized at factory default reset	Decrypt TLS master secret returned to module by Security Server after successful User authentication in support of

						802.11i EAP-TLS
3eTI Bridging Protocol Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
Bridging static key	AES ECB (e/d; 128,192,256) AES_CCM (128) TDES (Triple-DES 192)	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**
RSA private key	RSA (2048) (key wrapping; key establishment methodology provides 112-bits of encryption strength)	Not input (installed at factory)	Not output	Plaintext in flash	Zeroized when firmware is upgraded.	Used to support CO and Admin HTTPS interfaces.
TLS session key for encryption	Triple-DES (192) AES (128/192/256)	Not input, derived using TLS protocol	Not output	Plaintext in RAM	Zeroized when a page of the web GUI is served after it is used.	Used to protect HTTPS session.

The following is a table of cryptographic keys and key material that are unique to the product when it is operating in wireless Client mode:

Table 7 – SRDIs in Client Mode

Type	ID	Storage Location	Form	Zeroization
Certificate Authority (CA) public key certificate	"CA public key"	FLASH	Plaintext (inaccessible)	Zeroized when a new certificate is uploaded
Client public key certificate	Wpaclt.der	FLASH	Plaintext	Zeroized when a new certificate is uploaded
Client private key RSA (1024,2048,4092)	Wpaclt.pem	FLASH	Plaintext	Zeroized when a new certificate is uploaded

5. 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. Functional Specification is also provided.