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

3e-523-3
Secure Multi-function
Wireless Data Point

HW Versions 2.0(a)
FW Versions 4.5

Security Policy
Version 6.3

April 2016

Glossary of terms

AP	Access Point
CO	Cryptographic Officer
DHCP	Dynamic Host Configuration Protocol
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 product, the *3e-523-3 Secure Multi-function Wireless Data Point (3e-523-3)* (Hardware Versions: V2.0 (a); Firmware Versions: 4.5). This document defines 3eTI's security policy and explains how the 3e-523-3 meets the FIPS 140-2 security requirements.

In the FIPS mode of operation, the module secures all wireless communications with Wi-Fi Protected Access 2 (WPA2). WPA2 is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. The module uses the following cryptographic algorithm implementations:

- AES
- AES-CCM
- SHA-1
- HMAC SHA-1
- NIST SP800-90A DRBG
- RSA

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. The Cryptographic Module meets the overall FIPS 140-2 Level 2 requirement as detailed in the table below.

Table 1: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	3
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	N/A

1.2. Scope

This document covers the secure operation of the 3e-523-3, 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).

1.3. Cryptographic Module Definition

The 3e-523-3 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 standalone product. The module is physically bounded by the mechanical enclosure, which is protected by tamper evident tape. The physical cryptographic boundary of 3e-523-3 is defined to be the entire enclosure of the module.

The figure below shows the 523-3.

Figure 1 – 3e-523-3

2. Ports and Interfaces

The module provides one RJ45 Ethernet port and two RF antenna ports that connect to the same radio card inside the module.

Ethernet port is meant to be plugged into a secure IT environment. Data packets coming in and going out of RF antenna ports are encrypted by AES/AES-CCM depending on configuration.

a. Status output: Ethernet port and LED
b. Data output: Ethernet port and serial port and RF on antenna ports
c. Data input: Ethernet port and serial port and RF on antenna ports
d. Control input: Ethernet port and RF on antenna ports

The management interface of the Cryptographic Module (CM) uses HTTPS protocol. During the HTTPS session setup, the Cryptographic Module enforces mutual authentication between the web client and CM by requesting and validating the web client's certificate. The Cryptographic Officer must configure the CM with proper root certificate and OCSP server address to facilitate this mutual authentication between the web client and the CM.

3. Roles, Services, and Authentication

The 523-3 product supports user identity based operator authentication. There are total of three roles supported by the module. Two of which are operator roles and the other role is device role. Any operator user can belong to one of the operator roles. The operator user authenticates to the cryptographic module by using username and password and assumes his role upon successful authentication.

The set of services available to each role is defined in this section.

3.1.1. 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 other CO users and the Administrator users. The Crypto officer uses a secure mutually authenticated web-based HTTPS connection to configure the products and authenticates to the module using a username and password.

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 uses a secure mutually authenticated web-based HTTPS connection to configure the products and authenticates to the module using a username and password.

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

- Other Access Points (connecting in Bridge mode or when the CM is in wireless client mode)
- WLAN Client

When the product is configured to operate in Access Point/Bridge mode, the other device authenticates to the CM by using:

For Wireless client device:

The client proves its possession of the 256 bit PMK by performing 802.11i defined 4-way handshake protocol or proves its possession of the same encryption key for the static AES encryption mode.

For Bridge device:

The bridge device authenticates with the CM by proving the possession of the same encryption key. The key size is 128 for AES_CCM and 128,192 or 256 bit for AES encryption configuration

When the product is configured to operate in Wireless Client mode, the other device authenticates to the CM by using:

The other device (Access Point) through 802.11i defined 4-way handshake process proves that it has the same 256 bit PMK as the client obtained through EAP-TLS authentication from the RADIUS server, or manually input into the device.

The Device Role has access to the following services:

For Device Role (WLAN client)

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

For Device Role (AP)

- Apply Wireless Bridge Encryption on Data Packet
  - AES
  - AES_CCM
- Communicate with Wireless Client

- AES_CCM
- AES

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
Wireless Bridge													
• Encryption	AES_CCM (128 bit) AES (128-/192-256-bit)	X X	X X		X X	X X	X X						X X
Wireless Client													
• Security	PSK EAP-TLS Private Key Private Key Password		X X X		X X X	X X X	X X X						X X X

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
Monitoring / 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						

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.*

3.1.2. Authentication Mechanisms and Strength

The following table summarizes the roles and the type of authentication supported for each role:

Table 3 – Authentication versus Roles

Role	Type of Authentication	Authentication Data
Crypto Officer	ID-based	Crypto officers present unique usernames and passwords to log in to the module over HTTPS session. The HTTPS session enforces mutual authentication between the CM and the Web client
Administrator	ID-based	Admin officers present unique usernames and passwords to log in to the module over HTTPS session. The HTTPS session enforces mutual authentication between the CM and the Web client
Device Wireless client	static key or 802.11i authentication between wireless client and CM CM as Access Point	The possession of PMK or encryption key, if the PMK is manually entered to the CM, the passphrase mode is disallowed. Each wireless client is uniquely identified with its MAC address
AP	static key or 802.11i authentication between CM and AP (CM in wireless client mode)	The possession of the static key or the possession of PTK. Each AP is uniquely identified with its MAC address
AP	static key between CM and AP (CM in AP mode)	The possession of the static key. Each AP is uniquely identified with its MAC address.

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

Table 4 – 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
Shared secret	128 bits => 2^128 = 3.40E38
Bridging static key	128 bits => 2^128 = 3.40E38

4. 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.

4.1. 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. A compromised tape reveals message “OPENED” with visible red dots. 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.

8. The Crypto Officer shall login to make sure the device is in FIPS mode by logging in the Web UI and checking “Security Mode” in the page header. This header is available on every web GUI page.
9. The Crypto Officer shall not use an ASCII passphrase for the 802.11i PSK (Pre-Shared Key with Passphrase). Instead, the Crypto Officer must use either direct 802.11i PSK key input (Pre-Shared Key with Master Key) or EAP-TLS (802.1x) methods.
10. The Crypto Officer shall configure the CM to enforce mutual authentication between the Web Client and CM for remote management over HTTPs.

4.2. Physical Security Tamper Evidence

The 523-3 has weatherproof enclosure and is a stand-alone unit. The material used to cover the module is production grade and opaque within the visible spectrum.

The physical security provided is intended to provide 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.

The physical security provided is intended to provide FIPS 140-2 Level 2 physical security (i.e. tamper evidence).

The figures below show the physical interface sides of 3e-523-3 enclosure with tamper-evident seals.

Figure 2 – 3e-523-3 Physical Interface Side 1

Figure 3 – 3e-523-3 Physical Interface Side 2

5. Security Relevant Data Items

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

5.1. 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 0.9.7-beta3
AES; #1022
SHS: #976
RSA: #490
HMAC: #571
NIST SP800-90A DRBG: #1136

3e Technologies International Inc. 3eTI CryptoLib (Kernel Module) Algorithm Implementation 1.0
AES; #1021
SHS: #975
HMAC: #570
KTS (AES Cert. #1021 and HMAC Cert. #570; key establishment methodology provides between 128 and 256 bits of encryption strength)

3e Technologies International Inc. 3eTI Kernel Accelerated Crypto Core (Hardware) Algorithm Implementation 1.0
AES; #1023
SHS: #977
HMAC: #572

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
- Non-Approved RNG for approved DRBG seed and seed key generation

5.2 Self-tests

POST (Power on Self Test) is performed on each boot-time. On-demand self test is provided over the management interface. Crypto Officer User can command or schedule on-demand test from web GUI.

5.2.1 Power-on Self-tests

OpenSSL Power-on Self Tests

AES ECB - encrypt KAT
AES ECB - decrypt KAT
RSA - sign KAT
RSA - verify KAT
SHA-1 KAT
HMAC-SHA-1 KAT
NIST 800-90A DRBG KATs

Kernel Crypto Module Power-on Self Tests

AES ECB - encrypt KAT
AES ECB - decrypt KAT
AES CCM - encrypt KAT
AES CCM - decrypt KAT
SHA-1 KAT
HMAC-SHA-1 KAT

Kernel Crypto Coprocessor Power-on Self Tests (Hardware)

AES ECB - encrypt KAT
AES ECB - decrypt KAT
AES CCM - encrypt KAT
AES CCM - decrypt KAT
SHA-1 KAT
HMAC-SHA-1 KAT

Software Integrity Power-on Self Tests

HMAC-SHA-1 Integrity Test for firmware
HMAC-SHA-1 Integrity Test for bootloader

If any of the Power-on Self-tests fail, the system halts. The operator can attempt to power cycle the module to clear the error condition. Once the error condition has been cleared, the Crypto Officer or Administrator can view the logs to determine the type of failure.

5.2.2 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 wrapped in 3eTI proprietary format and HMAC-SHA1 hashed for integrity check.

Whenever a random number is generated (both NIST SP800-90A DRBG Approved and non-Approved), a Continuous Random Number Generator test is performed to ensure the random number is not repeating. DRBG health test is performed and both the DRBG seed and nonce are compared with previous ones to make sure they are not used consecutively.

5.2.3 Firmware Integrity Check by bootloader

After device is powered on, the first thing done by bootloader is to check firmware integrity. If the integrity fails, 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, too.

5.3 Cryptographic Keys and SRDIs

The module contains the following security relevant data items:

Table 5 - 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	Hash value in flash (PKCS#5)	Zeroized when reset to factory settings.	Used to authenticate CO and Admin role operators
Configuration file passphrase	HMAC key (ASCII string)	Input encrypted (using TLS session key) by Crypto Officer	Not output	Plaintext in RAM.	Zeroized when a configuration file is uploaded after it is used.	Used for downloaded configuration file message authentication
Firmware load key	HMAC key (ASCII string)	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 load message authentication
SNMP packet authentication	HMAC key (ASCII string)	Input encrypted	Not output	Ciphertext in flash	Zeroized when reset to	Use for SNMP

keys, username		(using TLS session key)			factory settings.	message authentication

RNG Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
DRBG CTR V	32-byte value	read from /dev/random which is hardware generated entropy	Not output	Plaintext in RAM	Zeroized every time a new random number is generated using the approved DRBG after it is used.	Used as CTR V value for Approved DRBG.
DRBG CTR Key	32-byte value	read from /dev/random which is hardware generated entropy	Not outut	Plaintext in RAM	Zeroized every time a new random number is generated using the approved DRBGafter it is used.	Used as CTR key for Approved DRBG.

3eTI Static Protocol Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
AP / Client Static key	AES ECB (e/d; 128,192,256)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash	Zeroized when encryption mode is changed or at factory default reset time	Used to encrypt unicast, and broadcast/ multitcast traffic in support of static mode

IEEE 802.11i Protocol Keys/CSPs (Common to PSK and EAP-TLS)						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
PMK	802.11i Pair-wise Master Key	Typed in 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	For 802.11i PSK mode, it's store in encrypted mode in flash For both 802.11i PSK and EAP-TLS, plaintext in RAM	Zeroized when authentication mode is changed If 802.11i PSK, zeroized when reset to factory settings.	802.11i PMK

PTK	AES (key derivation; 256)	Not input (derived from PMK)	Not output	Plaintext in RAM	When 802.11i session ends.	802.11i PTK
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
TK	AES CCM (e/d; 128)	Not input (derived from PTK)	Not output	Plaintext in RAM	When 802.11i session ends.	802.11i TK
TK (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
GMK	AES (key derivation; 256)	Not input (RNG)	Not output	Plaintext in RAM	Zeroized when authentication mode is changed When re-key period expires	802.11i GMK
GTK	AES CCM (e/d; 128)	Not input (derived from GMK)	Output encrypted (using KEK)	Plaintext in RAM	Zeroized when authentication mode is chagned 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	Zeroized when authentication mode changes Zeroied when reset to factory default	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	Zeroized when authentication mode changes Zeroied when reset to factory default	Authenticate messages between module and security server in support of 802.11i EAP-TLS
AES Key Wrap key	AES ECB key (d;128)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash	Zeroized when authentication mode changes Zeroied when	Decrypt TLS master secret returned to module by Security Server after

					reset to factory default	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)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash	Zeroized when bridge encryption mode is changed	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	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 table lists cryptographic keys and key material that are unique to the product when it is operating in wireless Client mode:

Table 6 – 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 2048	Wpaclt.pem	FLASH	Plaintext	Zeroized when a new certificate is uploaded