3e Technologies International, Inc.
FIPS 140-2
3e-523 and 3e-523-F1 WLAN Products
Non-Proprietary Security Policy
Level 2 Validation

Version 1.3

May 17, 2006

Glossary of terms

AP	Access Point
CO	Cryptographic Officer
DHCP	Dynamic Host Configuration Protocol
IP	Internet 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 *3e-523 and 3e-523-F1 WLAN Products* (Hardware Versions: 3e-523 V1.0 and 3e-523-F1 V1.0; Firmware Version: 3.4 Build 5), hereafter known as the 3e-523 / 3e-523-F1. This policy was created to satisfy the requirements of FIPS 140-2 Level 2. This document defines 3eTI's security policy and explains how the 3e-523 / 3e-523-F1 meets the FIPS 140-2 security requirements.

The figure below shows the 3e-523.

Figure A: 3e-523

The figure below show the 3e-523-F1

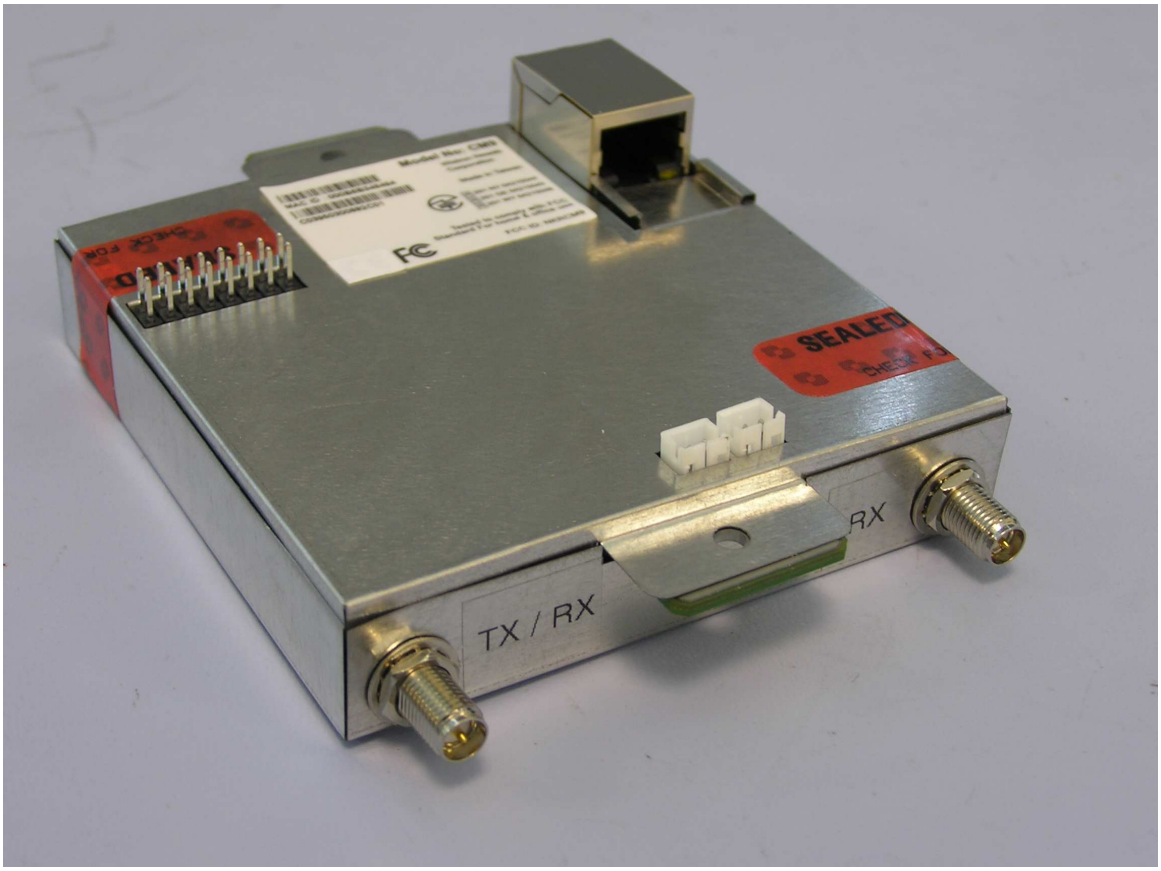

Figure B – 3e-523-F1

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/cryptval/.

1.2. Definition

The 3e-523 / 3e523-F1 is a device that consists of electronic hardware, embedded software and strong metal case. For purposes of FIPS 140-2, the module is considered to be a multi-chip standalone product. The 3e-523 / 3e-523-F1 operates as a Wireless Bridge for wired (LAN) networks. The cryptographic boundary of the 3e-523 and 3e-523-F1 is defined to be the entire enclosures of the 3e-523 and 3e-523-F1. Both the 3e-523 and the 3e-523-F1 enclosures are protected by tamper evident tape.

3e-523 / 3e-523F1 software provides the following major services in FIPS mode:

- Wireless 802.11a/b/g bridge functionality

- RS-232, RS-422 and RS-485 serial interface

1.3. Scope

This document will cover the secure operation of the 3e-523 / 3e-523-F1 including the initialization, roles and responsibilities of operating the product in a secure, FIPS-compliant manner, and describe the Security Relevant Data Items (SRDIs).

2. Roles, Services, and Authentication

The 3e-523 / 3e-523-F1 supports two separate roles. The set of services available to each role is defined in this section. The 3e-523 / 3e-523-F1 authenticates an operator's role by verifying his password.

2.1. Roles and Services

The 3e-523 / 3e-523-F1 supports the following authorized roles for operators:

Crypto Officer Role: The Crypto officer role performs all security functions provided by the Gateway. 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 must operate within the Security Rules and Physical Security Rules specified in Sections 3.1 and 3.2. The Crypto officer uses a secure web-based HTTPS connection to configure the Gateway. Up to ten Crypto Officers may be defined in the 3e-523 / 3e-523-F1. The Crypto Officer authenticates to the 3e-523 using a username and password.

Administrator Role: This role performs general configuration such as defining the WLAN, serial interface settings and viewing system log messages for auditing purposes. No CO security functions are available to the Administrator. The Administrator can also reboot the 3e-523 / 3e-523-F1 if deemed necessary.

The Administrator must operate within the Security Rules a specified in Section 3.1 and always uses a secure web-based HTTPS connection to configure the 3e-523/ 3e-523-F1. The Administrator authenticates to the 3e-523 / 3e-523-F1 using a username and password. Up to five operators who can assume the Administrator role can be defined. All Administrators are identical i.e. they have the same set of services available. The Crypto Officer is responsible for managing (creating, deleting) Administrator users.

The follow table outlines the functionalities that are provided by each role:

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[12]
System Configuration													
• General	Hostname	X	X				X	X	X				X
	Domain name	X	X				X	X	X				X
	Date/Time	X	X				X	X	X				X
• WAN	DHCP client	X	X				X	X	X				X
	Static IP address	X	X				X	X	X				X
	10/100 Mbps half/full duplex/auto	X	X				X	X	X				X
• Serial	RS-232, RS-422 and RS-485	X	X				X	X	X				X
Wireless Bridge Configuration													
• Bridging	Wireless Mode	X	X				X	X	X				X
	TX Rate	X	X				X	X	X				X
	Spanning Tree Protocol	X	X				X	X	X				X
	Channel No	X	X				X	X	X				X
	TX Pwr Mode	X	X				X	X	X				X
	Add/Remove Remote AP's BSSID	X	X				X	X	X				X
• Encryption	No Encryption	X	X				X						X
	TDES	X	X		X	X	X						X
	AES (128-/192-256-bit)	X	X		X	X	X						X
Service Settings													
• Generic IO		X	X				X						X
User Management													
• List All Users		X		X	X		X	X					X
• Add New User			X										
• User Password Policy	Enable/Disable	X	X				X						X
	Policy setting												
Monitoring/Reports													
• System Status	Security Mode	X						X					
	Current Encryption Mode	X						X					

[1] *The operator can view this setting*
[2] *The operator can change this setting*
[3] *The operator can add a required input. For example: Adding an entry to user list table*
[4] *The operator can delete a particular entry. For example: Deleting an entry from the user list table*
[5] *The operator can zeroize these keys.*
[6] *The operator can reset this setting to its factory default value. This is done by performing a zeroize*
[7] *The operator can view this setting*
[8] *The operator can change this setting*
[9] *The operator can add a required input. For example: Adding an to user list table*
[10] *The operator can delete a particular entry. For example: Deleting an entry from user list table*
[11] *The operator can zeroize these keys.*
[12] *The operator can reset this setting to its factory default value. This is done by performing a zeroize*

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[12]
	Bridging encryption mode	X						X					
	System Uptime	X						X					
	Total Usable memory	X						X					
	Free Memory	X						X					
	Current Processes	X						X					
	Other Information	X						X					
	Network interface status	X						X					
• Bridging Status	Status of Layer 2 bridge devices	X						X					
• Bridge Site Map	Map of bridge(s) within network												
• System Log	Date/Time/Message	X			X			X			X		
• Web Access Log		X			X			X			X		
• Network Activities		X			X			X			X		
System Administration													
• Firmware Upgrade		X											
• Self-Test		X						X					
• Factory Defaults		X											
• Reboot		X						X					
• Utilities	Ping	X						X					
	Traceroute	X						X					

2.2. Authentication Mechanisms and Strength

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

Role	Type of Authentication	Authentication Data
Crypto Officer	Role-based	Userid and password
Administrator	Role-based	Userid and password

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

Authentication Mechanism	Strength of Mechanism
Userid and password	Minimum 6 characters => 72^6 = 1.39E11

3. Secure Operation and Security Rules

In order to operate the 3e-523 / 3e-523-F1 securely, each operator should be aware of the security rules enforced by the module and should adhere to the physical security rules and secure operation rules detailed in this section.

3.1. Security Rules

The operator must follow the following 3e-523 / 3e-523-F1 security rules in order to ensure secure operation:

1. Every operator (Crypto Officer or Administrator) has a user-id on the 3e-523./ 3e-523-F1 No operator will violate trust by sharing his/her password associated with the user-id with any other operator or entity.
2. The Crypto Officer will not share any key, or SRDI used by the 3e-523 / 3e-523-F1 with any other operator or entity.
3. The operators will explicitly logoff by closing all secure browser sessions established with the 3e-523./ 3e-523-F1
4. The operator will disable browser cookies and password storing mechanisms on the browser used for web configuration of the device.
5. The Crypto officer is responsible for inspecting the tamper evident seals on a daily basis. 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 should change the default password when configuring the 3e-523 / 3e-523-F1 for the first time. The default password should not be used.

3.2. Physical Security Rules

The following section contains detailed instructions to the Crypto Officer concerning where and how to apply the tamper evident seals to the 3e-523 / 3e-523-F1 enclosure, in order to provide physical security for FIPS 140-2 level 2 requirements.

Tools:

Wire Cutters (wire seal removal)

Materials:

3e-523, 3e-523F1– Quantity: 1
Seal, Tape, Tamper-evident – Quantity: 2
Isopropyl Alcohol Swab
3M Adhesive Remover (citrus or petroleum based solvent)

Installation – Tamper-evident tape

1. Locate on 3e-523/3e-523-F1 the placement locations of tamper-evident tape seals. (2 locations as shown in Figure 1 and 2 for the 3e-523 and Figure 1b and 2b for the 3e-523-F1).

2. Thoroughly clean area where tamper-evident tape seal is to be applied with isopropyl alcohol swab. Area must be clean of all oils and foreign matter (dirt, grime, etc.)
3. Record tracking number from tamper-evident tape seal.
4. Apply seal to locations on the 3e-523 as shown in Figures 1 and 2 and to the 3e-523-F1 as shown in Figures 1b and 2b. It is important to ensure that the seal has equal contact area with both top and bottom housings.
5. After application of seals to 3e-523/3e-523-F1, apply pressure to verify that adequate adhesion has taken place.

Removal – Tamper-evident tape

1. Locate on 3e-523/3e-523-F1 locations of tamper-evident tape seals. (2 locations as shown in Figures 1 and 2 for the 3e-523 and Figure 1b and 2b for the 3e-523-F1)
2. Record tracking numbers from existing tamper-evident tape seal and verify physical condition as not tampered or destroyed after installation.
3. Cut tape along seam of 3e-523/3e-523-F1 to allow opening of enclosure.
4. Remove nut and washer from antenna connectors.
5. Using 3M adhesive remover or equivalent, remove residual tamper-evident seal tape. (two locations as shown in Figures 1 and 2 for the 3e-523 and Figure 1b and 2b for the 3e-523-F1)

This picture shows the physical interface side of 3e-523 enclosure with tamper-evident seal.

Figure 1

Front-view of 3e-523 showing LAN port, LEDs and tamper-evident seal:

Figure 2

These pictures below show the physical interface side of 3e-523-F1 enclosure with tamper-evident seal.

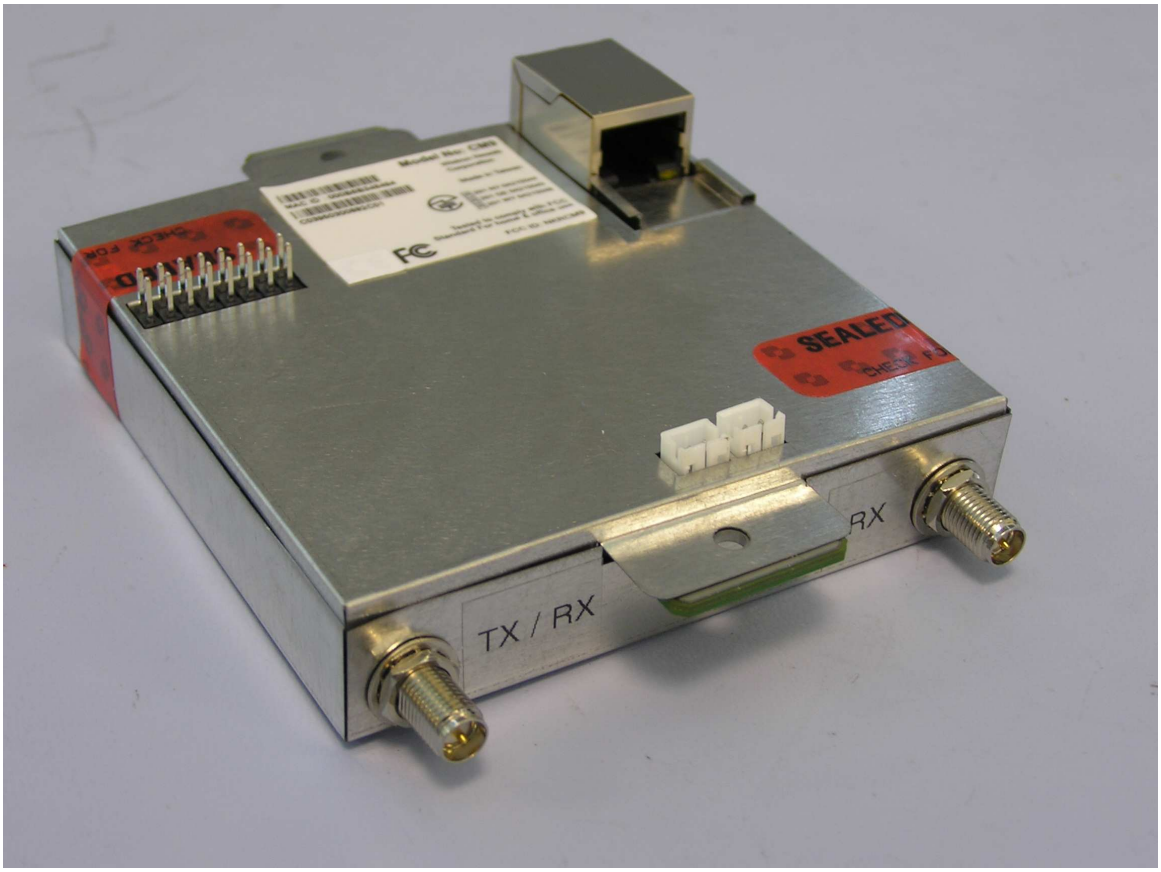

Figure 1b

Figure 2b

3.3. Secure Operation Initialization

Refer to the 3e-523/3e-523-F1 User Manual for details of secure operation initialization and screen shots. The module always operates in a FIPS Approved mode and does not have a non-Approved mode.

4. Security Relevant Data Items

This section specifies the 3e-523's / 3e-523-F1's Security Relevant Data Items (SRDIs) as well as the access control policy enforced by the 3e-523 / 3e-523-F1.

3.4. Cryptographic Algorithms

The 3e-523/3e-523F1 supports the following FIPS Approved cryptographic algorithms:

- TDES (ECB, CBC modes; 192-bit keysize)
- AES (ECB mode; 128, 192, 256-bit keysizes)
- SHA-1
- HMAC-SHA1
- RNG (FIPS 186-2, SHA-1 based)

The 3e-523/3e-523F1 also supports the following non-FIPS cryptographic algorithms:

- RSA decrypt (PKCS#1 using a 1024-bit modulus) allowed in FIPS mode for key un-wrapping. This key establishment method provides 80-bits of security.

3.5. Self-tests

- Power-up Self-tests
  - TDES ECB - encrypt/decrypt KAT
  - TDES CBC - encrypt/decrypt KAT
  - AES ECB - encrypt/decrypt KAT
  - SHA-1 KAT
  - HMAC-SHA-1 KAT
  - Bootloader Image Integrity Test
  - FIPS 186-2 (Appendix 3.1, 3.3) KAT
  - Integrity Test for firmware

- Conditional Self-tests
  - CRNGT for Approved PRNG
  - CRNGT for non-Approved PRNG (Open SSL based)
  - Bypass Test
  - Firmware Load Test

3.6. Cryptographic Keys and SRDIs

The 3e-523 / 3e-523-F1 contains the following security relevant data items:

Type	ID	Storage Location	Form	Zeroizable	Zeroization Mechanism	Function
Plaintext Keys						
AES ECB 256 bit	"AES internal key to encrypt config file"	FLASH	Plaintext (inaccessible)	Y	Zeroized by upgrading firmware	To protect the configuration file
RNG Seed Key 160 bit	"RNG seed key"	RAM	Plaintext (inaccessible)	Y	Zeroized immediately following use (after function is called and returned)	To generate the RNG
RSA Private Key	"HTTPS/TLS RSA private key"	FLASH	Plaintext (inaccessible)	Y	Zeroized by upgrading firmware	N/A
HMAC-SHA-1 key (1)	"firmware integrity check key for firmware load test"	FLASH	Plaintext (inaccessible, hard-coded)	Y	Zeroized by upgrading firmware	N/A
TLS Session Key	"HTTPS/TLS session key"	RAM	Plaintext (inaccessible)	Y	When the module is powered down.	N/A
Web-GUI logon password for the Crypto Officer	"CO web-GUI logon password"	FLASH	Hashed using SHA-1	Y	Setting the module to factory default	CO logon credential.
Web-GUI logon password for the Administrator	"Admin web-GUI logon password"	FLASH	Hashed using SHA-1	Y	Setting the module to factory default	Admin logon credential.
Downloaded configuration file password	"downloaded config file pwd"	RAM	Plaintext (inaccessible)	Y	Immediately following use	To protect the configuration file
Encrypted Keys: These keys are stored encrypted in the module and as such do not require zeroization.						
AES Static 128,192, or 256 bit	"static AES key"	FLASH	Encrypted AES using "system config AES key"	N/A	N/A	Wireless Bridging
TDES Static 192 bit	"static TDES key"	FLASH	Encrypted AES using "system config AES key"	N/A	N/A	Wireless Bridging

3.7. Access Control Policy

The 3e-523 / 3e-523-F1 maintains and enforces the access control policy for each SRDI stored within the module. These access control policies cannot be changed or modified by any role within the module. The permissions are categorized as a set of three separate permissions: read (R), write (W), execute (E). If no permission is listed, then the operator cannot access the SRDI. The following table defines the access that an operator has to each SRDI and through which services.

3e-523/3e-523-F1 SRDI Roles and Services Access Policy	Security Relevant Data Item	AES or TDES Static Key	AES Internal Key	HMAC SHA-1 Key	RNG Seed Key	TLS Session Key	RSA Private Key	Crypto-officer password	Administrator Password	Downloaded Config File Password
Role/Service										
Crypto-officer Role										
System Configuration			E			E	E			E
Wireless Configuration		W	E			E	E			
Service Settings			E			E	E			
User Management						E	E	W	W	
Monitoring/Reporting			E			E	E			
System Administration			E	E		E	E			
Administrator Role										
System Configuration			E			E	E			
Wireless Configuration			E			E	E			
Service Settings			E			E	E			
User Management						E	E		W	
Monitoring/Reporting			E			E	E			
System Administration			E			E	E			