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

3e-523-F2 Secure Multi-function Wireless Data Point

Version 2.1

September 2007

Glossary of terms

AP	Access Point
CO	Cryptographic Officer
DH	Diffie Hellman
DHCP	Dynamic Host Configuration Protocol
DMZ	De-Militarized Zone
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
NAT	Network Address Translation
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-F2 Secure Multi-function Wireless Data Point (3e-523-F2)* (Hardware Versions: HW V1.0, V1.1; Firmware Version 4.1.7.2). 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-F2 meets the FIPS 140-2 security requirements.

The figure below shows the 3e-523-F2.

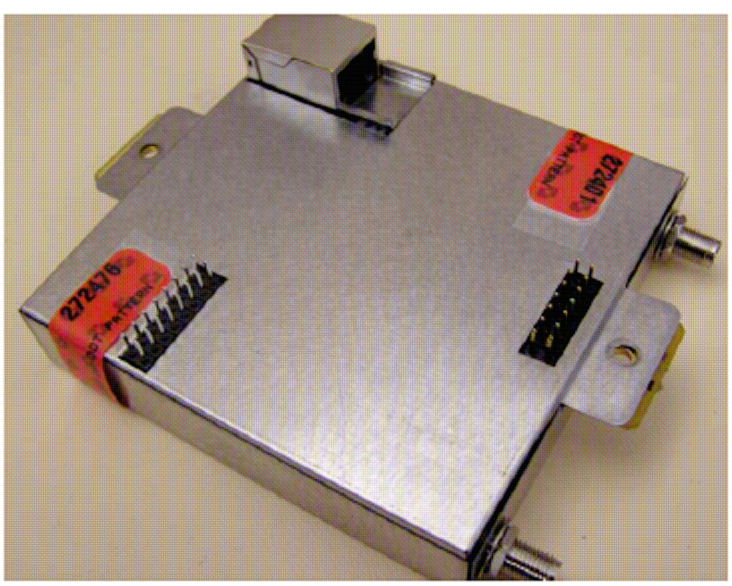

Figure 1 – 3e-523-F2

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-F2 is a device, which 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-F2 operates as either a gateway connecting a local area network to wide area network (WAN), an access point within a wireless local area network (WLAN), a client within a WLAN, or a wireless bridging device. The

cryptographic boundary of the 3e-523-F2 is defined to be the entire enclosure of the Product. The 3e-523-F2 is physically bound by the mechanical enclosure, which is protected by tamper evident tape.

3eTI software provides the following major services in FIPS mode:

- Wireless 802.11a/b/g Access Point functionality
- Wireless 802.11a/b/g Client functionality
- Wireless 802.11a/b/g Bridge functionality (bridging from the wired uplink LAN to the wireless LAN).
- Wireless 802.11a/b/g functionality (auto-forming, self-healing wireless capability)
- DHCP service to the local LAN (allows a wired local LAN to exist over the local LAN interface).
- SNMP*
- USB compatibility
- Subnet Roaming
- Virtual LAN
- 802.11i
- 2Mbits Boot FLASH, 16 MB FLASH, 64 MB SDRAM

When the 3e-523-F2 is in Client mode, a Configuration Utility provides an intuitive user interface to configure, manage and use various features. The administrator can configure up to 10 separate profiles. Each profile consists of various wireless configuration parameters like:

Security Mode (FIPS or non-FIPS mode)
SSID
Card type (802.11a/b/g)
Wireless authentication type
Encryption (AES, Triple-DES, DKE, AES-CCMP) and related keys or certificate.
Power level
Transmit rate.

* Although SNMP traffic is transmitted encrypted (using DES or AES), for FIPS purposes, it is considered to be plaintext. The reason being, encryption keys are derived from a pass-phrase, which is not allowed in FIPS mode.

1.3. Scope

This document will cover the secure operation of the 3e-523-F2 including the initialization, roles and responsibilities of operating the product in a secure, FIPS-compliant manner, and describe the Security Relevant Data Items (SRDIs).

The 3e-523-F2 has six modes of operations, which are listed in the table below:

Mode	FIPS Mode
Gateway Mode (Mode 1)	No
Gateway Mode (Mode 2)	Yes
AP / Bridging Mode (Mode 1)	No
AP / Bridging Mode (Mode 2)	Yes
Client Mode (Mode 1)	No
Client Mode (Mode 2)	Yes

2. Roles, Services, and Authentication

The 3e-523-F2 supports four separate roles. The set of services available to each role is defined in this section. The 3e-523-F2 authenticates an operator's role by verifying his PIN or access to a shared secret.

2.1.1. Roles & Services

The 3e-525A-3 supports the following authorized roles for operators:

Crypto Officer Role: The Crypto officer role performs all security functions provided by the 3e-523-F2. 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 3e-523-F2. Up to ten Crypto Officers may be defined in the 3e-523-F2. The Crypto Officer authenticates to the 3e-523-F2 using a username and password.

Administrator Role: This role performs general 3e-523-F2 configuration such as defining the WLAN, LAN and DHCP settings, performing self-tests 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-F2, 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-F2. The Administrator authenticates to the 3e-523-F2 using a username and password. Up to 5 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 following table outlines the functionalities that are provided by the "operator" roles (Crypto Officer and Administrator):

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
• LAN	IP address	X	X				X	X	X				X
	Subnet mask	X	X				X	X	X				X
• Operating Mode	Gateway – FIPS	X	X				X	X	X				X
	Gateway – Non-FIPS	X	X				X	X	X				X
	AP / Bridging Mode – FIPS	X	X				X	X	X				X
	AP / Bridging Mode – Non-FIPS	X	X				X	X	X				X
	AP / Bridging Mode – FIPS / IPv6												
	AP / Bridging Mode – Non-FIPS / IPv6												
Wireless Access Point													
• General	SSID	X	X				X	X	X				X
	Wireless Mode	X	X				X	X	X				X
	Channel Number	X	X				X	X	X				X
	• Enable / Disable	X	X				X	X	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 the MAC address filtering table*
[4] *The operator can delete a particular entry. For example: Deleting an entry from the MAC address filtering 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 entry to the MAC address filtering table*
[10] *The operator can delete a particular entry. For example: Deleting an entry from the MAC address filtering 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]
	Auto Selection	X	X				X	X	X				X
	• Auto selection	X	X				X	X	X				X
	button	X	X				X	X	X				X
	Transmit Power Mode	X	X				X	X	X				X
	Fixed Power Level	X	X				X	X	X				X
	Beacon Interval	X	X				X	X	X				X
	RTS Threshold	X	X				X	X	X				X
	DTIM	X	X				X	X	X				X
	Basic Rates	X	X				X	X	X				X
	Preamble												
	Enable / Disable Broadcast SSID												
• Security	No Encryption	X	X				X						X
	Dynamic Key	X	X				X						X
	Management	X	X			X	X						X
	Triple-DES	X	X			X	X						X
	AES (128-/192-256-bit)	X	X				X						X
	FIPS 802.11i												
• Wireless VLAN	Enable/Disable	X	X				X						X
	VLAN	X	X	X	X	X	X						X
• MAC Address Filtering	Enable/Disable	X	X				X	X					X
	Add/Delete entry			X	X								
	Allow/Disallow Filter	X	X				X	X					X
• Rogue AP Detection	Enable/Disable	X	X				X	X	X				X
	Known AP MAC			X	X								
	address	X	X				X	X	X				X
	Email / Display rogue AP												
• Advanced	Load Balancing	X	X				X	X	X				X
	Layer 2 Isolation	X	X				X	X	X				X
Wireless Bridge													
• General	Manual/Auto Bridge	X	X				X	X	X				X
	SSID	X	X				X	X	X				X
	Max Auto Bridge	X	X				X	X	X				X
	Bridge Priority	X	X				X	X	X				X
	Signal Strength	X	X				X	X	X				X
	Threshold	X	X				X	X	X				X
	Broadcast SSID	X	X				X	X	X				X
	enable/disable	X	X				X	X	X				X
	Signal Strength LED	X	X		X		X	X	X		X		X
	MAC												
	STP enable/disable												
	Remote BSSID												
• Radio	Wireless Mode	X	X				X	X	X				X
	Tx Rate	X	X				X	X	X				X
	Channel No	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[12]
	Tx Pwr Mode	X	X				X	X	X				X
	Propagation Distance	X	X				X	X	X				X
	RTS Threshold	X	X				X	X	X				X
	Remote BSSID			X						X			
• Encryption	No Encryption	X	X				X						X
	Triple-DES	X	X		X	X	X						X
	AES (128-/192-256-bit)	X	X		X	X	X						X
Service Settings													
• DHCP Server	Enable / Disable	X	X				X	X	X				X
	Starting / Ending IP address	X	X				X	X	X				X
• Subnet Roaming	Enable / Disable	X	X				X	X	X				X
	Coordinator Address	X	X		X		X	X	X	X			X
• SNMP agent	Enable/ Disable	X	X				X	X	X				X
	Community settings	X	X				X	X	X				X
	Secure User Configuration	X	X				X	X	X				X
	System Information	X	X				X	X	X				X
• Misc Service	Print Server: Enable/ Disable	X	X				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	X	X				X						X
Monitoring/Reports													
• System Status	Security Mode	X						X					
	Current Encryption Mode	X						X					
	Bridging encryption mode	X						X					
	System Uptime	X						X					
	Total Usable memory	X						X					
	Free Memory	X						X					
	Current Processes	X						X					
	Other Information												
	Network interface status												
• Bridging Status	Status of Layer 2 bridge devices	X						X					
• Wireless Clients	MAC Address (manfr's name)	X						X					
	Received Signal Strength	X						X					
	TX rate												

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]
• Adjacent AP List	AP MAC address SSID Channel Signal Noise Type Age WEP	X X X X X X X X						X X X X X X X X					
• DHCP Client List	Client Hostname IP Address MAC Address (manfr's name)	X X X			X X X			X X X			X X X		
• System Log	Date/Time/Message	X			X			X			X		
• Web Access Log		X			X			X			X		
• Network Activities		X			X			X			X		
Auditing													
• Log		X					X	X					X
• Report Query		X						X					
• Configuration	Enable/Disable Selectable items	X X	X X				X X						X X
System Administration													
• System Upgrade	Firmware Upgrade Local Configuration Upgrade Remote Configuration Upgrade	X X X	X X X				X X X						X X X
• Factory Defaults		X											
• Remote Logging	Enable/Disable Settings	X X	X X				X X	X X	X X				X X
• Reboot		X						X					
• Utilities	Ping Traceroute	X X						X X					

Client Role: The Client Role is the User Role. This role is assumed by the wireless client workstation that uses static or dynamic key AES or Triple-DES encryption to communicate wirelessly with the 3e-523-F2 when the 3e-523-F2 is in AP mode. Authentication is implicitly selected by the correct knowledge of the static key, or for dynamic key encryption, EAP-TLS authentication is performed and the client uses its

public key certificate to authenticate itself. The static key (TDES or AES key) is configured on the 3e-523-F2 by the Crypto officer. The static key must be pre-shared between the 3e-523-F2 and the client. The 3e-523-F2 supports 128 clients / client workstations, if MAC address filtering is disabled. If MAC address filtering is enabled, only 60 clients are allowed.

The Client role has the ability to send data to and through the 3e-523-F2. All data is sent in the form of 802.11 wireless packets. All wireless communication is encrypted using either Triple-DES or AES encryption (based upon the 3e-523-F2 configuration). In bypass mode, plaintext packets can also be sent to the 3e-523-F2. The Client role also employs 802.11i authentication schemes including 802.1X, EAP-TLS, and preshared key modes. Also, a Wireless Access Point (WAP) may act in the Client role by communicating with the 3e-523-F2 in bridging mode.

A slight variant of the Client role is when the 3e-523-F2 is in Client mode and is associating to an external wireless access point.

Security Server Role: This role is assumed by the authentication server, which is a self-contained workstation connected to the 3e-523-F2 over the Ethernet Uplink WAN port. The security server is employed for authentication of wireless clients and key management activities. The Security Server is used only during dynamic key exchange. The Security Server authenticates using a shared secret which is used as an HMAC-SHA1 key to sign messages sent to the 3e-523-F2 during dynamic key exchange. The Security Server IP address and password are configured on the 3e-523-F2 by the Crypto Officer. Only one Security Server is supported.

The Security Server performs following services:

- EAP-TLS authentication
- Process dynamic key exchange after a successful authentication
- Perform a DH key exchange with the 3e-523-F2 to negotiate an AES key
- Send Unicast key to the Gateway encrypted with the AES key negotiated using a DH key exchange

2.1.2. Authentication Mechanisms and Strength

The following table summarizes the four 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
Client	Role-based	Static Key (TDES or AES)
Client	Role-based	CA signature
Client	Role-based	AES CCM pre-shared key
Security Server	Role-based	HMAC SHA1 (Shared secret)

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

Authentication Mechanism	**Strength of Mechanism**
Userid and password	Minimum 8 characters => 94^8 = 6.096E15
Static Key (TDES or AES)	TDES (192-bits) or AES (128, 192, or 256-bits)
HMAC SHA-1 shared secret	Minimum 10 characters => 94^10 = 5.386E19
CA signature	Modulus size1024 bits (provides 80 bits of strength)
AES CCM pre-shared key	Minimum 8 characters => 94^8 = 6.096E15
EAP-TLS	CA signature => Modulus size 1024 bits (provides 80 bits of strength)

3. Secure Operation and Security Rules

In order to operate the 3e-523-F2 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 following 3e-523-F2 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 3e-523-F2. 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-F2 with any other operator or entity.
3. The Crypto Officer will not share any MAC address filtering information used by the 3e-523-F2 with any other operator or entity.
4. The operators will explicitly logoff by closing all secure browser sessions established with the 3e-523-F2.
5. The operator will disable browser cookies and password storing mechanisms on the browser used for web configuration of the 3e-523-F2.
6. 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.
7. The Crypto Officer should change the default password when configuring the 3e-523-F2 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-F2 enclosure, in order to provide physical security for FIPS 140-2 level 2 requirements.

Tools:

Wire Cutters (wire seal removal)

Materials:

3e-523-F2– 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-F2 the placement locations of tamper-evident tape seals. (Locations as shown in Figure 2).
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-F2 as shown in Figure 2. 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-F2, apply pressure to verify that adequate adhesion has taken place.

Removal – Tamper-evident tape

1. Locate on 3e-523-F2 locations of tamper-evident tape seals (2 locations as shown in Figure 2).
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-F2 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 Figure 2).

The picture below shows the physical interface side of 3e-523-F2 enclosure with tamper-evident seals.

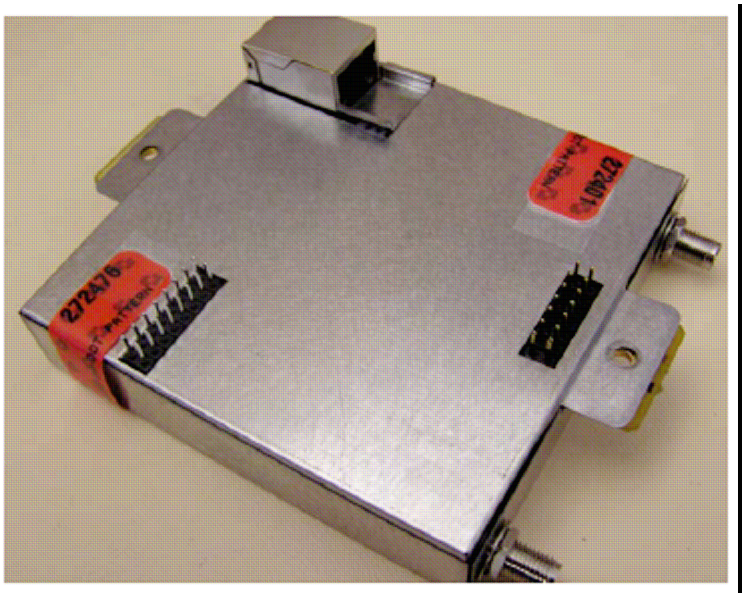

Figure 2

3.3. Secure Operation Initialization

Refer to the 3e-523-F2 User Manual for details of secure operation initialization and screen shots.

1. The operator will disable browser cookies and password storing mechanisms on the browser used for web configuration of the 3e-523-F2.
2. The CO will change the default CO password that is shipped with the module.
3. The CO will apply tamper evidence labels as described in section 3.2 above.
4. The CO will select the FIPS mode of operation radio button.
    a. In order to enter FIPS mode, select the FIPS 140-2 Mode box on the Operation Mode page of the management GUI. This will force the 3e-523-F2 to return to factory defaults and then the unit will reboot into FIPS mode. To leave FIPS mode, un-select the FIPS 140-2 Mode box and apply the changes. Once again, the 3e-523-F2 will restore factory defaults and then reboot into non-FIPS mode.
    b. On transition between modes, the system is returned to factory defaults.

4. Security Relevant Data Items

This section specifies the 3e-523-F2's Security Relevant Data Items (SRDIs) as well as the access control policy enforced by the 3e-523-F2.

4.1. Cryptographic Algorithms

The 3e-523-F2 supports the following FIPS-approved cryptographic algorithms:

- TDES (ECB, CBC modes; 192-bit key size)
- AES (ECB mode; 128, 192, 256-bit key sizes)
- AES CCM (128-bit key size)
- SHA-1
- HMAC-SHA1
- FIPS 186-2 (Appendix 3.1 and 3.3) PRNG
- RSA Sign/Verify

The 3e-523-F2 also supports the following non-FIPS cryptographic algorithms:

- Diffie Hellman (1024-bit modulus) allowed in FIPS mode for key agreement. This key establishment method provides 80-bits of security.
- RSA (key wrapping, key establishment methodology provides 80 bits of encryption strength)
- RC4 (used in WEP/WPA)
- MD5 hashing (used in MS-CHAP for PPPoE and SNMP agent)
- DES CBC (non-compliant) (used in SNMP v3)
- AES CFB (non-compliant) (used in SNMP v3)

4.2 Self-tests

4.2.1 Power-up Self-tests

Triple-DES ECB - encrypt/decrypt KAT

AES ECB - encrypt/decrypt KAT

Triple-DES CBC – encrypt/decrypt KAT

AES CCM KAT

SHA-1 KAT

HMAC-SHA-1 KAT

FIPS 186-2 (Appendix 3.1, 3.3) RNG KAT

SHA-1 Integrity Test for firmware

RSA Sign/Verify

4.2.2 Conditional Self-tests

CRNGT for Approved PRNG

CRNGT for non-Approved PRNG (Open SSL based RNG)

Bypass Test

Firmware Load Test using HMAC-SHA-1

4.2.3 Critical Functions tests

DH pairwise consistency test (power-up)

4.3 Cryptographic Keys and SRDIs

The following is a list of all cryptographic keys and key components used by the 3e-523-F2 when in wireless AP, Bridge, or Client mode:

Type	ID	Storage Location	Form	Zeroizable	Zeroization Mechanism	Function
Plaintext Keys						
PMK 256 bit	"pairwise master key"	RAM	Plaintext (inaccessible)	Y	By changing the mode to FIPS-11i or static key encryption	Master key used to derive PTK
GMK 256 bit	"group master key"	RAM	Plaintext (inaccessible)	Y	By changing the mode to FIPS-11i or static key encryption	Master key used to derive GTK
AES Dynamic Broadcast 128,192, or 256 bit	"dynamic broadcast AES key"	RAM	Plaintext (inaccessible)	Y	By changing the mode to FIPS-11i or static key encryption	Client Access
Triple-DES Dynamic Broadcast 192 bit	"dynamic broadcast Triple-DES key"	RAM	Plaintext (inaccessible)	Y	By changing the mode to FIPS-11i or static key encryption	Client Access
AES Dynamic Unicast 128,192, or 256 bit	"dynamic unicast AES key"	RAM	Plaintext (inaccessible)	Y	By changing the mode to FIPS-11i or static key encryption	Client Access
Triple-DES	"dynamic	RAM	Plaintext	Y	By changing the	Client Access

Dynamic Unicast 192 bit	unicast Triple-DES key"		(inaccessible)		mode to FIPS-11i or static key encryption	
RNG Seed Key 160 bit	"RNG seed key"	RAM	Plaintext (inaccessible)	Y	Zeroized immediately following use (after function is called & returned)	To generate the RNG
AES post-authentication 256 bit	"post - authentication AES key"	RAM	Plaintext (inaccessible)	Y	Zeroized after the unicast key (encrypted by this AES key) is decrypted by the module	This key is used to AES encrypt the unicast key used by our legacy DKE functionality
AES-CCM Dynamic Broadcast 128 bit **(GTK)**	"dynamic broadcast AES-CCM key use for FIPS-11i"	RAM	Plaintext (inaccessible)	Y	By changing encryption mode to DKE or static key encryption	Client Access
KCK 128 bit	"key MIC key"	RAM	Plaintext (inaccessible)	Y	By changing encryption mode to DKE or static key encryption	To generate MIC in 802.11i key message
KEK 128 bit	"key encryption key"	RAM	Plaintext (inaccessible)	Y	By changing encryption mode to DKE or static key encryption	To encrypt GTK in 802.11i key message
AES-CCM Dynamic Unicast 128 bit **(TK)**	"dynamic unicast AES-CCM key use for FIPS-11i"	RAM	Plaintext (inaccessible)	Y	By changing encryption mode to DKE or static key encryption	Client Access
802.11i pre-shared passphrase 8 to 63 chars	"802.11i pre-shared passphrase"	RAM	Plaintext (inaccessible)	Y	By changing the mode to FIPS-11i or static key encryption	Used to generate PMK
RSA Private Key	"HTTPS/TLS RSA private key"	FLASH	Plaintext (inaccessible)	Y	Setting the module to factory default	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
HMAC-SHA-1 key (3)	SNMP packet authentication key	FLASH	Plaintext	Y	Setting the module to factory default	N/A
TLS Session Key	"HTTPS/TLS session key"	RAM	Plaintext (inaccessible)	Y	When the module is powered down.	N/A
Diffie-Hellman Private	"diffie-hellman prime"	RAM	Plaintext	Y	Zeroized after the unicast key	N/A

Exponent, 1024-bit					(encrypted by the established AES key) is decrypted by the module	
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.
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	Client Access
AES Static 128,192, or 256 bit	"static AES key"	FLASH	Encrypted AES using "system config AES key"	N/A	N/A	Wireless Bridging
Triple-DES Static 192 bit	"static Triple-DES key"	FLASH	Encrypted AES using "system config AES key"	N/A	N/A	Client Access
Triple-DES Static 192 bit	"static Triple-DES key"	FLASH	Encrypted AES using "system config AES key"	N/A	N/A	Wireless Bridging
HMAC-SHA-1 key (2)	"backend HMAC key"	FLASH	Encrypted AES using "system config AES key"	N/A	N/A	Used for keyed authentication between the Security Server and the 523-F2 when the 523-F2 is acting as an Access Point
802.11i TLS Key Encryption Key	"backed AES key"	FLASH	Encrypted AES using "system config AES key"	Y	Setting the module to factory default	To encrypt Transport TLS Session Key
Downloaded configuration file password	"downloaded config file pwd"	FLASH	Encrypted AES using "system config AES key"	N/A	N/A	To protect the configuration file

The following is a table of cryptographic keys and key material that are unique to the 3e-523-F2 when it is operating in wireless Client mode:

Type	ID	Storage Location	Form	Zeroizable
AES CCM Passphrase 8 to 63 bytes	"AES CCM Passphrase"	RAM	Encrypted AES using "system config AES key"	Y
AES Static 128 bit	"system config	Hard coded in source	Plaintext, used to encrypt the	Y

Type	ID	Storage Location	Form	Zeroizable
	AES key"		real static Aes/Triple-DES keys (inaccessible, hard-coded) and passwords	
RSA Public Key	"EAP/TLS RSA certificate"	FLASH	Plaintext (inaccessible)	Y
Certificate Authority (CA) public key certificate	"CA public key"	FLASH	Plaintext	N
EAP-TLS Pre-Master Key 48-byte	"dynamic session pre-master key"	RAM	Plaintext (inaccessible)	Y

4.4 Access Control Policy

The 3e-523-F2 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), and 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, used by the 3e-523-F2 when in wireless AP, Bridge, or Client mode:

3e-523-F2 SRDI Roles & Services Access Policy (AP, Bridge, Client modes)	CO – System Configuration	CO – Wireless Configuration	CO – Service Settings	CO – User Management	CO – Monitoring / Reporting	CO – System Administration	AD – System Configuration	AD – Wireless Configuration	AD – Service Settings	AD – User Management	AD – Monitoring / Reporting	AD – System Administration	User Role – Sending Data	AS Role – Provides Authentication
PMK 256 bit														
GMK 256 bit														
AES Dynamic Broadcast 128,192, or 256 bit													E	
Triple-DES Dynamic Broadcast 192 bit													E	
AES Dynamic Unicast 128,192, or 256 bit													E	
Triple-DES Dynamic Unicast													E	

192 bit														
RNG Seed Key 160 bit														
AES post-authentication 128 bit														W
AES-CCM Dynamic Broadcast 128 bit **(GTK)**													E	
KCK 128 bit													E	
KEK 128 bit													E	
AES-CCM Dynamic Unicast 128 bit **(TK)**													E	
802.11i pre-shared passphrase 8 to 63 chars		W						W						
RSA Private Key	E	E	E	E	E	E	E	E	E	E	E	E		
HMAC-SHA-1 key (1)						E								
HMAC-SHA-1 key (3)						E								
TLS Session Key	E	E	E	E	E	E	E	E	E	E	E	E		
Diffie-Hellman Private Exponent, 1024-bit														
Web-GUI logon password for the Crypto Officer	W													
Web-GUI logon password for the Administrator	W						W							
AES Static 128,192, or 256 bit		W											E	
AES Static 128,192, or 256 bit		W											E	
Triple-DES Static 192 bit		W											E	
Triple-DES Static 192 bit		W											E	

HMAC-SHA-1 key (2)														
802.11i TLS Key Encryption Key		W											E	
Downloaded configuration file password						W								

The following table defines the access that an operator has to each SRDI and through which services, used by the 3e-523-F2 when in wireless Client mode:

3e-523-F2 SRDI Roles & Services Access Policy (Client mode)	**CO – System Configuration**	**CO – Wireless Configuration**	**CO – Service Settings**	**CO – User Management**	**CO – Monitoring / Reporting**	**CO – System Administration**	**AD – System Configuration**	**AD – Wireless Configuration**	**AD – Service Settings**	**AD – User Management**	**AD – Monitoring / Reporting**	**AD – System Administration**	**User Role – Sending Data**	**AS Role – Provides Authentication**
AES CCM Passphrase 8 to 63 bytes	W													
AES Static 128, 192, or 256 bit	W													
Triple-DES Static 192 bit	W													
AES Dynamic Broadcast 128,192, or 256 bit													E	
Triple-DES Dynamic Broadcast 192 bit													E	
AES Dynamic Unicast 128,192, or 256 bit													E	
Triple-DES Dynamic Unicast 192 bit													E	
AES Static 128 bit	W													

HMAC SHA-1 Key	W											E	
RSA Public Key													W
RSA Private Key	E	E	E	E	E	E	E	E	E	E	E		W
CryptoOfficer Password	W												
Admin Password	W												
Certificate Authority (CA) public key certificate													E
AES-CCM Dynamic Groupcast 128 bit												E	
AES-CCM Unicast 128 bit												E	
AES Static 128 bit												E	
EAP-TLS Pre-Master Key 48 byte													E