3e Technologies International, Inc.
FIPS 140-2
Non-Proprietary Security Policy
Level 2 Validation
3e-527A3 AirGuard[TM] Wireless Access Point,
3e-527A3 AirGuard[TM] Wireless Access Point with Outdoor Option, and
3e-527A3MP AirGuard[TM] Wireless Access Point with Mobile Power

Version 7.0

November 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 gateway product with the following variations:

3e-527A3 AirGuard**TM** Wireless Access Point
HW V1.1, Firmware Version 4.0.10.23

3e-527A3 AirGuard**TM** Wireless Access Point with Outdoor Option
HW V1.1, Firmware Version 4.0.10.23

3e-527A3MP AirGuard**TM** Wireless Access Point with Mobile Power
HW V1.1, Firmware Version 4.0.10.23

See section 3.2 of this document for an overview of the differences among the (3) variations. 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 (3) 3e-527A3 variations meet the FIPS 140-2 security requirements. Unless otherwise stated, "3e-527A3" in this document refers to all (3) 527A3 variations.

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-527A3 is a device, which consists of electronic hardware, firmware and strong metal case. For purposes of FIPS 140-2, the module is considered to be a multi-chip standalone product. The 3e-527A3 operates as either a gateway connecting a local area network to wide area network (WAN) or as an access point within a local area network (LAN). The cryptographic boundary of the 3e-527A3 is defined to be the entire enclosure of the Gateway. The 3e-527A3 is physically bound by the mechanical enclosure, which is protected by tamper evident tape.

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

-   Wireless 802.11b/g Access Point functionality (bridging from the wired uplink LAN to the wireless LAN).
-   Wireless 802.11a bridge functionality
-   DHCP service to the local LAN (allows a wired local LAN to exist over the local LAN interface).

- SNMP*
- Subnet Roaming
- 802.11i
- 64MB SDRAM Xscale Card Revision D and Revision E.
- Firewall (gateway mode only)
  - DNS Proxy
  - NAT (IP Filtering, Port Filtering, Port Forwarding, DMZ)
  - Stateful Packet Inspection
  - Blocking ICMP/SNMP from WAN
  - Blocking URL by domain name
  - Blocking DNS query request

1.3.   Scope

This document will cover the secure operation of the 3e-527A3 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 527A3 has two modes of operations, which are listed in the table below:

Mode	FIPS Mode
Gateway Mode (Mode 1)	Yes
AP /Bridging Mode (Mode 2)	Yes

The 527A3 always operates in FIPS-mode.

---

* Although SNMP traffic is transmitted obfuscated (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.

2. Roles, Services, and Authentication

The 3e-527A3 supports four separate roles. The set of services available to each role is defined in this section. The 3e-527A3 authenticates an operator's role by verifying his PIN or access to a shared secret. The 3e-527A3 does not support any unauthenticated roles.

2.1 Roles and Services

The 3e-527A3 supports the following authorized roles for operators:

Crypto Officer Role: The Crypto officer role performs all security functions provided by the 3e-527A3. 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-527A3. Up to ten Crypto Officers may be defined in the 3e-527A3. The Crypto Officer authenticates to the 3e-527A3 using a username and password.

Administrator Role: This role performs general 3e-527A3 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-527A3, 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-527A3. The Administrator authenticates to the 3e-527A3 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
	Domain name	X	X					X	X				X
	Date/Time	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
	AP / Bridging Mode – FIPS	X	X					X	X	X			X
	AP / Bridging Mode – FIPS / IPv6	X	X					X	X	X			X
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 Auto Selection	X	X					X	X	X			X
	• Auto selection 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	X	X					X	X	X			X
	Enable / Disable Broadcast SSID	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	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]
• Security	Dynamic Key Management	X					X						X
	Triple-DES	X	X			X	X						X
	AES (128-/192-256-bit)	X	X			X	X						X
	FIPS 802.11i	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 address			X	X								
	Email / Display rogue AP	X	X				X	X	X				X
• Advanced	Load Balancing	X	X				X	X	X	X			X
	Layer 2 Isolation	X	X				X	X	X	X			X
Wireless Bridge													
• General	Manual/Auto Bridge	X	X				X	X	X	X			X
	SSID	X	X				X	X	X	X			X
	Max Auto Bridge	X	X				X	X	X	X			X
	Bridge Priority	X	X				X	X	X	X			X
	Signal Strength Threshold	X	X				X	X	X	X			X
	Broadcast SSID enable/disable	X	X				X	X	X	X			X
	Signal Strength LED MAC	X	X				X	X	X	X			X
	STP enable/disable	X	X				X	X	X	X			X
	Remote BSSID	X	X		X		X	X	X	X	X		X
• Radio	Wireless Mode	X	X				X	X	X	X			X
	Tx Rate	X	X				X	X	X	X			X
	Channel No	X	X				X	X	X	X			X
	Tx Pwr Mode	X	X				X	X	X	X			X
	Propagation Distance	X	X				X	X	X	X			X
	RTS Threshold	X	X				X	X	X	X			X
	Remote BSSID			X							X		
• Encryption	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			X
	Starting / Ending IP address	X	X				X	X	X	X			X
• Subnet Roaming	Enable / Disable	X	X				X	X	X	X			X
	Coordinator Address	X	X		X		X	X	X	X	X		X
• SNMP agent[13]	Enable/ Disable	X	X				X	X	X	X			X
	Community settings	X	X				X	X	X	X			X
	User Configuration	X	X				X	X	X	X			X
	System Information	X	X				X	X	X	X			X
User Management													
• List All Users		X		X	X		X	X					X
• Add New User			X										

---

[13] Although SNMP traffic is transmitted obfuscated (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.

Version 7.0

Categories	Features	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]
Operator Roles — CryptoOfficer / Administrator													
• 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	X						X					
	Network interface status	X						X					
• 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	X						X					
• Adjacent AP List	AP MAC address	X						X					
	SSID	X						X					
	Channel	X						X					
	Signal	X						X					
	Noise	X						X					
	Type	X						X					
	Age	X						X					
	WEP	X						X					
• DHCP Client List	Client Hostname	X			X			X			X		
	IP Address	X			X			X			X		
	MAC Address (manfr's name)	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
• Report Query		X											
• Configuration	Enable/Disable	X	X				X						X
	Selectable items	X	X				X						X
System Administration													
• System Upgrade	Firmware Upgrade	X	X				X						X
	Local Configuration Upgrade	X	X				X						X
	Remote Configuration Upgrade	X	X				X						X
• Factory Defaults							X						X
• Remote Logging	Enable/Disable	X	X				X	X	X				X
	Settings	X	X				X	X	X				X
• Reboot		X	X					X	X				
• Utilities	Ping	X						X					
	Traceroute	X						X					

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-527A3. Mutual authentication using EAP-TLS is performed between the client workstation and the security server, where the 527A3 device operates in pass-through mode. EAP-TLS certificate authentication is NOT performed by the 527A3 device itself; rather, the client workstation and security server are EAP-TLS endpoints, and the 527A3 device simply passes EAP-TLS traffic between the client and security server endpoints.

The User role has the ability to send data to and through the 3e-527A3. 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-527A3 configuration). The User role also employs 802.11i authentication schemes (between client and security server endpoints with 527A3 acting in pass-through mode) including 802.1X, EAP-TLS, and preshared key modes. Also, a Wireless Access Point (WAP) may act in the User role by communicating with the 3e-527A3 in bridging mode.

Security Server Role: This role is assumed by the authentication server, which is a self-contained workstation connected to the 3e-527A3 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-527A3 during dynamic key exchange. The Security Server IP address and password are configured on the 3e-527A3 by the Crypto Officer. Only one Security Server is supported.

The Security Server performs following services:

- The EAP-TLS authentication from 3e-SS through the 3e-WAP to the 3e-010F Crypto Client
- Process dynamic key exchange after a successful authentication
- Perform a DH key exchange with the 3e-527A3 to negotiate an AES key
- Send Unicast key to the Gateway encrypted with the AES key negotiated using a DH key exchange

AES Keywrap is another way of transporting the key from RADIUS server to Access Point. The key is encrypted using AES Key Wrap algorithm and transported to AP using the RADIUS protocol. The AES Key Wrap Encryption Key is a 128-bit key manually inputted on both AP and RADIUS server side. The entire RADIUS packet is protected by HMAC-SHA1 algorithm, where the HMAC-SHA1 password is manually inputted on both AP and RADIUS server side.

2.2 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
User	Role-based	Static Key (TDES or AES)
User	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 10 characters => $94\text{^}10 = 5.386E19$
Static Key (TDES or AES)	TDES (192-bits) or AES (128, 192, or 256-bits)
HMAC SHA-1 shared secret	Minimum 10 characters => $94\text{^}10 = 5.386E19$
AES CCM pre-shared key	Minimum 8 characters => $94\text{^}8 = 6.095E15$

2.3 Bypass Mode

The 3e-527A3 provides the capability of a Bypass mode. This mode can be set only by the Crypto-Officer role. Selecting this mode results in giving the User role the ability to send data to and from the 3e-527A3 in unencrypted form.

3. Secure Operation and Security Rules

In order to operate the 3e-527A3 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-527A3 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-527A3. 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-527A3 with any other operator or entity.
3. The Crypto Officer will not share any MAC address filtering information used by the 3e-527A3 with any other operator or entity.
4. The operators will explicitly logoff by closing all secure browser sessions established with the 3e-527A3.
5. The operator will disable browser cookies and password storing mechanisms on the browser used for web configuration of the 3e-527A3.
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-527A3 for the first time. The default password should not be used.

3.2. Physical Security Rules

Difference between the versions of 3e-527A3 Product:

1. All 3 versions use the same firmware.
2. All 3 versions use the same radios and the same antennae.
3. The Standard Version (3e-527A3) (a) has an externally-accessible switch, (b) has a reset-switch that is physically accessed through one of the Ethernet ports, and (c) the unit is powered by PoE (Power over Ethernet).
4. The Mobile Power Version (3e-527A3MP) (a) has an externally-accessible switch, (b) has a reset-switch that is physically accessed through one of the Ethernet ports, and (c) the unit is powered by a 9-36V DC power.
5. The Standard with OUTDOOR OPTION Version (3e-527A3) (a) does not have an externally-accessible switch – only the 3 standard RJ-45 Ethernet ports that are available on all versions but with water-tight connectors on this version , (b) does not have a reset-switch that is physically accessed through one of the Ethernet

ports but does have a reset function that is accessible through a the ENCRYPT port, and (c) the unit is powered by PoE (Power over Ethernet).

The following section contains detailed instructions to the Crypto Officer concerning where and how to apply the tamper evident seals to the 3e-527A3 enclosure, in order to provide physical security for FIPS 140-2 level 2 requirements.

A security seal is added from the back plate to the antenna plate. A second security seal is added from the front of the unit to the antenna plate, taking care not to cover the L.E.D. labeling. A ½" 440 Pan Head screw replaces one of the 5/8" 4-40 Pan Head screws on the circular connector used for power input for the 527A3-MP. Then two 440 KEPS nuts are added and tightened together with washers facing each other approximately 1/32" from the PEM. This prevents the screws from being removed and thus entry cannot be obtained without removing the security labels. Add Security Seal from the flat of the antenna connector to the front side of unit. A second security seal is added from the back plate of the unit to the antenna plate.

Tools:
        Wire Cutters (wire seal removal)
Materials:
        3e-527A3 – Quantity: 1
        Seal, Tape, Tamper-evident – Quantity: 4
        Isopropyl Alcohol Swab
        3M Adhesive Remover (citrus or petroleum based solvent)

Installation – Tamper-evident tape

1. Locate on 3e-527A3 the placement locations of tamper-evident tape seals.
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 the 3e-527A3. It is important to ensure that the seal has equal contact area with both top and bottom housings.
5. After application of seals to the 3e-527A3, apply pressure to verify that adequate adhesion has taken place.

Removal – Tamper-evident tape

1. Locate on 3e-527A3 locations of tamper-evident tape seals.
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-527A3 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.

Location of Tamper-evident Tape

Figure 1. 3e-527A3 Standard – Antenna Panel

Figure 2. 3e-527A3 Standard – I/O Panel
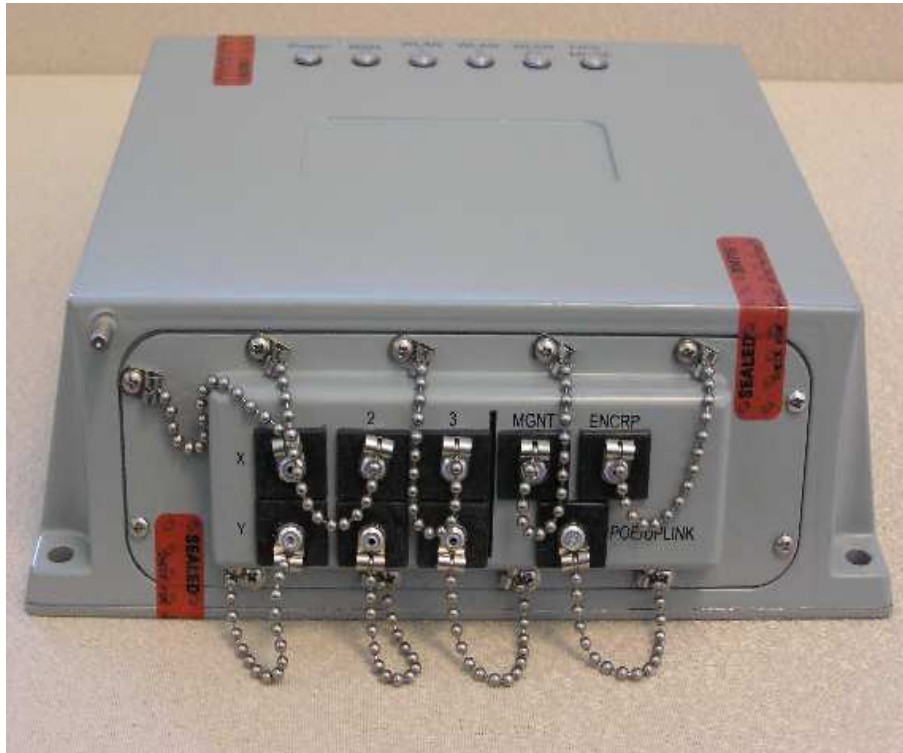
Figure 3. 3e-527A3MP Antenna Panel

Figure 4. 3e-527A3MP– I/O Panel

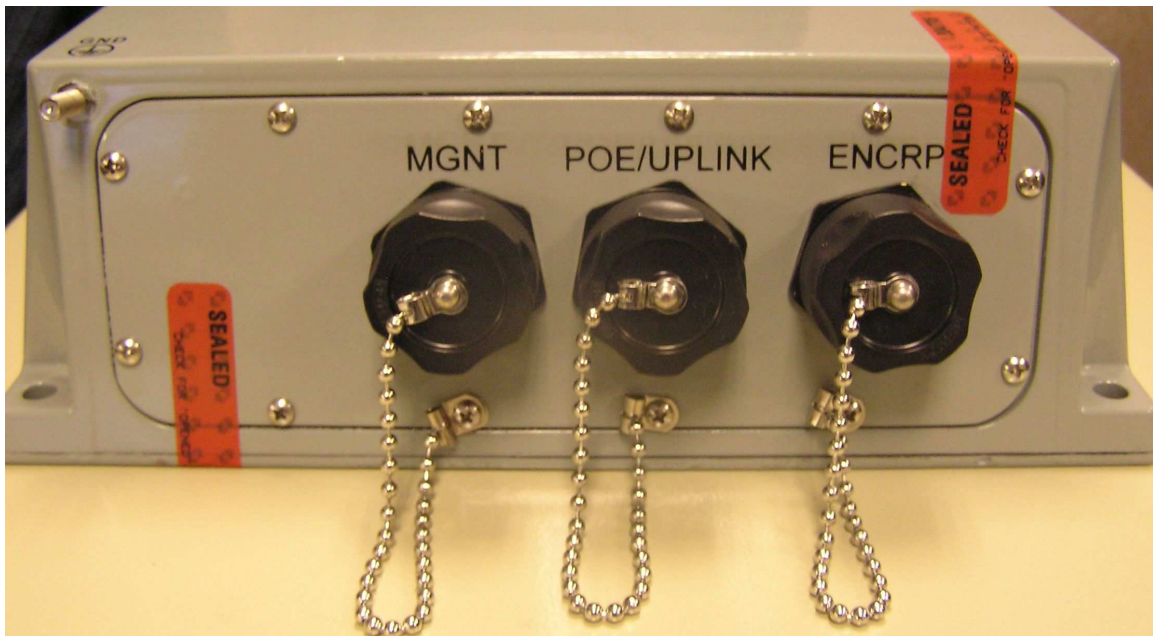**Figure 5. 3e-527A3 W/OUTDOOR OPTION – Antenna Panel**

Figure 6. 3e-527A3 W/OUTDOOR OPTION – I/O Panel

3.3.   *Secure Operation Initialization*

Refer to the 3e-527A3 User Manual for details of secure operation initialization and screen shots.

Version 7.0

20

4. Security Relevant Data Items

This section specifies the 3e-527A3's Security Relevant Data Items (SRDIs) as well as the access control policy enforced by the 3e-527A3.

4.1. Cryptographic Algorithms

The 3e-527A3 supports the following FIPS-approved cryptographic algorithms:

- TDES (ECB, CBC modes; 192-bit keysize)
- AES (ECB mode; 128, 192, 256-bit keysizes)
- AES CCM (128-bit keysize)
- SHA-1
- HMAC-SHA1
- FIPS 186-2 (Appendix 3.1 and 3.2) PRNG

The 3e-527A3 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 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.
- 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

AES CFB   - 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

4.2.2 Conditional Self-tests

CRNGT for Approved PRNG

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

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 3e-527A3 contains the following security relevant data items:

Type	ID	Storage Location	Form	Zeroizable	Zeroization Mechanism	Function
Plaintext Keys						
AES ECB 256 bit	"system config AES key"	FLASH	Plaintext (inaccessible)	Y	Zeroized by upgrading firmware	To encrypt/decrypt the "encrypted" 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 Unicast 192 bit	"dynamic unicast Triple-DES key"	RAM	Plaintext (inaccessible)	Y	By changing the mode to FIPS-11i or static key encryption	Client Access

Type	ID	Storage Location	Form	Zeroizable	Zeroization Mechanism	Function
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 128 bit	"post - authentication AES key"	RAM	Plaintext (inaccessible)	Y	Zeroized after the unicast key (encrypted by this AES key) is decrypted by the module	N/A
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
Downloaded configuration file password	"downloaded config file pwd"	RAM	Plaintext (inaccessible)	Y	Zeroized immediately following use (after function is called & returned)	To protect the configuration file when downloaded
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

Version 7.0

Type	ID	Storage Location	Form	Zeroizable	Zeroization Mechanism	Function
Diffie-Hellman Private Exponent, 160-bit	"diffie-hellman prime"	RAM	Plaintext	Y	Zeroized after the unicast key (encrypted by the established AES key) is decrypted by the module	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.
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	N/A
HMAC-SHA-1 key (4)	"DKE HMAC key"	FLASH	Encrypted AES using "system config AES key"	N/A	N/A	N/A
802.11i TLS Key Encryption Key	"backend AES key"	FLASH	Encrypted AES using "system config AES key"	Y	Setting the module to factory default	To encrypt Transport TLS Session Key

4.4 Access Control Policy

The 3e-527A3 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.

3e-527A3 SRDI Roles & Services Access Policy	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 192 bit													E	
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	

	1	2	3	4	5	6	7	8	9	10	11	12	13
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, 160-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)		W											
HMAC-SHA-1 key (4)		W											
802.11i TLS Key Encryption Key		W										E	
Downloaded configuration file password					W								