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

3e-525A-3,
3e-525A-3 BASIC,
3e-525A-3 BASIC with TEC,
3e-525A-3MP,
3e-525A-3MP with TEC
AirGuard™ Wireless Access Points

HW Version 2.0(A), 2.0(A), 2.0(A), 2.0(A), 2.0(A)
FW Version 4.2.1.23

Security Policy Version 1.1

August 1, 2008

1. INTRODUCTION 1

2. REFERENCES 1

3. AIRGUARD WIRELESS ACCESS POINT 2

3.1. CRYPTOGRAPHIC MODULE 2
3.2. MODULE INTERFACES 4
3.3. ROLES AND SERVICES 5
3.3.1. Crypto Officer and Administrator Role Services 6
3.3.2. User Role Services 10
3.3.3. Security Server Role Services 10
3.3.4. Unauthenticated Services 11
3.4. CRYPTOGRAPHIC ALGORITHMS 12
3.5. CRYPTOGRAPHIC KEYS AND SRDIS 12
3.6. SELF-TESTS 19
3.7. SECURE OPERATION OF THE AIRGUARD WIRELESS ACCESS POINT 20
3.7.1. Applying Tamper-Evident Seals (All Models) 20
3.7.2. Checking for Tamper Evidence 25

GLOSSARY 26

1. Introduction

This document describes the non-proprietary cryptographic module security policy for 3e Technologies International's wireless gateway product variations, the *3e-525A-3, 3e-525A-3 BASIC, 3e-525A-3 BASIC with TEC, 3e-525A-3MP, 3e-525A-3MP with TEC AirGuard™ Wireless Access Points* (Hardware Versions: 2.0(A), 2.0(A), 2.0(A), 2.0(A), 2.0(A); Firmware Version: 4.2.1.23). 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 gateway product variations meet the FIPS 140-2 security requirements.

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/.

2. References

- *AirGuard™ Wireless Access Point User's Guide*, Model 3e-525A-3, Model 3e-525A-3 Basic, Model 3e-525A-3MP, 6/3/08.
- *Installation Guide for the 3e525A-3MP Wireless Access Point with Mobile Power*, document Revision A.

3. AirGuard Wireless Access Point

3.1. Cryptographic Module

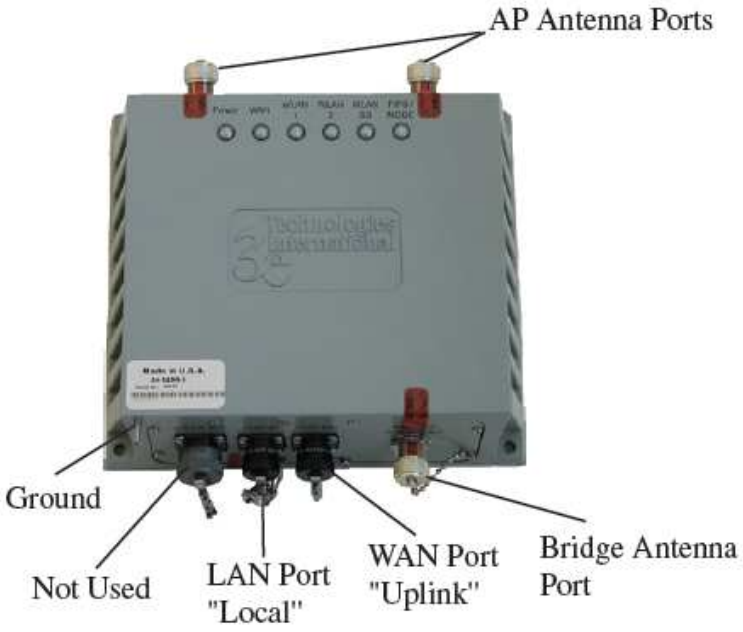
The five variants of the 525A-3 AirGuard Wireless Access Point module (the module) are devices, which consist of electronic hardware, embedded software and strong metal case. There are two different types of metal cases, one for non-MP models, and one for MP models, as depicted in the figures below. For purposes of FIPS 140-2, the module is considered to be a multi-chip standalone product. The five variants of the module differ from each other as follows:

1. 525A-3 has mil-spec-461 compliant filters. Uses Power Over Ethernet (POE).
2. 525A-3 BASIC does not have the mil-spec-461-compliant filtering. Uses POE.
3. 525A-3 BASIC w/TEC is a variant of #2 above with a thermo-electric cooler installed.
4. 525A-3MP has power (24V nominal) entering through the antenna panel.
5. 525A-3MP w/TEC is a variant of #4 above with a thermo-electric cooler installed.

The term *TEC* in two of the variants stands for *Thermo-Electric Cooler*. It is circuitry included within the unit to extend the temperature range of the unit. It is used to pump heat energy away from the WLAN circuit boards to the enclosure case in warm environment.

The module 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 module is defined to be the entire enclosure of the Gateway. The module is physically bound by the mechanical enclosure, which is protected by tamper evident tape.

525A-3 metal case



525A-3MP models' power port on AP Antennae panel

3.2. Module Interfaces

There are three modes of operation that determine how antennae and ports are used by the module:

- Mode #1. Access point mode
  - Local antennae (2) configured to encrypt/decrypt
  - LAN port used for administration
  - WAN port used to connect protected wired network
  - Bridging antenna – configurable
- Mode #2. Gateway mode
  - local antennae (2) configured to encrypt/decrypt
  - LAN port used to connect protected wired network
  - WAN port used to connect unprotected external network
  - Either LAN or WAN port used for administration.
  - Bridging antenna – configurable
- Mode #3. Bridging mode:
  - Bridge antenna configured to encrypt/decrypt
  - Local antennae (2) may be configured for either access point mode or bridging mode.

Additionally, there is no separate power port for the "-3" models (they use Power over Ethernet a.k.a. PoE), while there is a separate DC power port for the "MP" models.

The following table summarizes module interfaces when the module is operating in access point mode:

FIPS interface	Module interface
Data input	Local antennae (2)
	Bridging antenna (if enabled)
	WAN port
Data output	Local antennae (2)
	Bridging antenna (if enabled)
	WAN port
Control input	LAN port
Status output	LEDs: • Power • WAN • WLAN 1 • WLAN 2 • WLAN SS • FIPS/MODE
	LAN port
Power port	WAN port (PoE)

	MP port (DC)

The following table summarizes module interfaces when the module is operating in gateway mode:

FIPS interface	Module interface
Data input	Local antennae (2)
	Bridging antenna (if enabled)
	LAN port
	WAN port
Data output	Local antennae (2)
	Bridging antenna (if enabled)
	LAN port
	WAN port
Control input	LAN port
	WAN port
Status output	LEDs: • Power • WAN • WLAN 1 • WLAN 2 • WLAN SS • FIPS/MODE
	LAN port
	WAN port
Power port	WAN port (PoE)
	MP port (DC)

3.3. Roles and Services

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

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

Authentication Mechanism[1]	Strength of Mechanism
Userid and password	Minimum 8 characters => 94^8 = 1.641E-16
Static Key (TDES or AES)	TDES (192-bits) or AES (128, 192, or 256-bits)
AES CCM pre-shared key	Minimum 8 characters => 94^8 = 6.095E15

The module halts (introduces a delay) for a second after each unsuccessful authentication attempt by CO or Admin. The highest rate of authentication attempts to the module is one attempt per second. This translates to 60 attempts per minute. Therefore the probability for multiple attempts to use the module's authentication mechanism during a one-minute period is 60/(94^8), or less than (9.84E-15).

3.3.1. Crypto Officer and Administrator Role Services

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

Administrator Role: This role performs general module 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 module, 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 module. The Administrator authenticates to the module 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.

[1] *The module implements one authentication mechanism that authenticates individual operators into Crypto Officer and Administrator roles: the web GUI username/password mechanism. The module implements three authentication mechanisms that implicitly authenticate operators into a single User operator role: 3eTI static pre-shared key mechanism, 802.11i pre-shared key mechanism, 3eTI bridging pre-shared key mechanism. The module relies on an authentication server in the environment to authenticate User operators for 3eTI DKE and 802.11i EAP-TLS Approved encrypting modes.*

Crypto Officer and Administrator services, and the keys/CSPs that each role has access to using web GUI page to provide correspondence to the key/CSP are summarized in the table below. If there is no web GUI interface to input/output a key/CSP, neither the Crypto Officer nor the Administrator have access to it. Please see the table titled "RFC 2818 HTTPS Keys/CSPs" under section 3.5 of this document for a list of keys/CSPs used/generated as a result of executing the Web GUI service..

Categories	Features	Operator Roles									
		CryptoOfficer					Administrator				
		Show[2]	Set[3]	Add[4]	Delete[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Default Reset[11]
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	X	X			X	X	X			X
	AP / Bridging Mode – Non-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	X	X			X	X	X			X

[2] *The operator can view this setting*
[3] *The operator can change this setting*
[4] *The operator can add a required input. For example: Adding an entry to the MAC address filtering table*
[5] *The operator can delete a particular entry. For example: Deleting an entry from the MAC address filtering table*
[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. 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 reset this setting to its factory default value.*

Categories	Features	Operator Roles									
		CryptoOfficer					Administrator				
		Show[2]	Set[3]	Add[4]	Delete[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Default Reset[11]
	Selection										
	• 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
• Security	No Encryption	X	X			X					X
	Dynamic Key Management	X	X			X					X
	Triple-DES	X	X			X					X
	AES (128-/192-256-bit)	X	X			X					X
	FIPS 802.11i	X	X			X					X
• Wireless VLAN	Enable/Disable	X	X			X					X
	VLAN	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 address			X	X						
	Email / Display rogue AP	X	X			X	X	X			X
• 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 Threshold	X	X			X	X	X			X
	Broadcast SSID enable/disable	X	X			X	X	X			X
	Signal Strength LED MAC	X	X			X	X	X			X
	STP enable/disable	X	X		X	X	X	X		X	X
	Remote BSSID	X	X			X	X	X			X
• 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
	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

Categories	Features	Operator Roles									
		CryptoOfficer					Administrator				
		Show[2]	Set[3]	Add[4]	Delete[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Default Reset[11]
	AES (128-/192-256-bit)	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	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										
• 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	

Categories	Features	Operator Roles									
		CryptoOfficer					Administrator				
		Show[2]	Set[3]	Add[4]	Delete[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Default Reset[11]
• 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				

3.3.2. User Role Services

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 module. Authentication is either performed through entry of a static key by the user or an EAP-TLS authentication is performed, with the user providing a public key certificate. The static key (TDES or AES key) is configured on the module by the Crypto officer. The static key must be pre-shared between the module and the User. The Gateway supports 128 Users (client workstations) if MAC address filtering is disabled. If MAC address filtering is enabled, only 60 Users are allowed.

The User role has the ability to send data to and through the module. All data is sent in the form of 802.11i wireless packets. All wireless communication is encrypted using either Triple-DES or AES encryption (based upon the module's configuration). In bypass mode, plaintext packets can also be sent to the module. The User 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 User role by communicating with the module in bridging mode.

3.3.3. Security Server Role Services

Security Server Role: This role is assumed by the authentication server, which is a self-contained workstation connected to the module 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 module during dynamic key exchange. The Security Server IP address and password are configured on the module 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 module to negotiate an AES key
- Send Unicast key to the Gateway encrypted with the AES key negotiated using a DH key exchange

3.3.4. Unauthenticated Services

Unauthenticated services include the following:

Service	Description	Input	Output	Key/CSP
802.11a/b/g (and variants, as well as WLAN management functions such as VLAN and MAC filtering are supported as described in the *User's Guide* section "Introduction")	802.11 wireless traffic (used in both Approved encrypting modes and in bypass modes)	802.11a/b/g inputs and data	802.11a/b/g outputs and data	None
NAT	Wired network service available only in gateway mode (used in both Approved encrypting modes and in bypass modes)	NAT inputs and data	NAT outputs and data	None
DHCP	Wired network service available only in gateway	DHCP inputs and data	DHCP outputs and data	None

	mode (used in both Approved encrypting modes and in bypass modes)			

3.4. Cryptographic Algorithms

The module supports the following FIPS-approved cryptographic algorithms:

- TDES (ECB, CBC modes; 192-bit keysize), cert #292
- AES (ECB mode; 128, 192, 256-bit keysizes), cert #238
- AES CCM (128-bit keysize), cert #1
- SHA-1, cert #278
- HMAC-SHA1, cert #13
- FIPS 186-2 (Appendix 3.1 and 3.1) PRNG, cert#22

The module 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.
- 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)

3.5. Cryptographic Keys and SRDIs

The module contains the following security relevant data items:[12]

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	Ciphertext in flash (SHA-1 hash)	Not zeroized	Used to authenticate CO and Admin role operators
Configuration file	HMAC key (ASCII string)	Input encrypted	Not output	Plaintext in RAM. It is put	Zeroized when a	Used for downloaded

[12] *There is in addition to the keys/CSPs listed below a "configuration file key". However, it is not considered either a key or a CSP. Keys/CSPs encrypted using the configuration file key stored in flash are considered stored as plaintext.*

passphrase		(using TLS session key)		into temporary memory/auto variable/stack.	configuration file is uploaded after it is used.	configuration file message authentication
Firmware integrity check key	HMAC key (ASCII string)	Input encrypted (using TLS session key)	Not output	Plaintext in flash	Not zeroized.	Used for firmware load message authentication
SNMP packet authentication keys, username	HMAC key (ASCII string)	Input encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when reset to factory settings.	Use for SNMP message authentication
RNG Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
FIPS 186-2 seed	ASCII string (includes the value of a call to the standard C library time() function)	Not input	Not output	Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS PRNG after it is used.	Used to initialize FIPS PRNG
FIPS 186-2 seed key	Symmetric	RNG	Not output	Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS PRNG after it is used.	Used to initialize FIPS PRNG
3eTI Static Protocol Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
Static key	1. AES ECB (e/d; 128,192,256) 2. TDES (Triple-DES 192)	Input encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when local antennae Approved encrypting mode either reconfigured or changed from 3eTI Static mode to any other local antennae Approved encrypting mode, to bypass mode. Zeroized when reset to factory settings.	Used to encrypt unicast, and broadcast/ multitcast traffic in support of static mode
3eTI DKE Protocol Keys/CSPs						

Key/CSP	Type	Generation/ Input	Output	Storage	Zeroization	Use
See EAP-TLS keys/CSPs	-	-	-	-	-	There are DKE-specific EAP-TLS keys/CSPs used to authenticate User operator to module
Dynamic unicast key	1. AES ECB (e/d; 128,192,256) 2. TDES (Triple-DES 192)	Not input (TLS master secret resulting from successful User EAP-TLS authentication in DKE mode)	Not output	Plaintext in RAM	Zeroized when 3eTI DKE session times out Note that it takes approximately five minutes for a DKE session to time out given the DKE protocol specification. When a timeout occurs after a session times out, zeroization is immediate.	Used to encrypt unicast traffic in support of DKE
Dynamic broadcast key	1. AES ECB (e/d; 128,192,256) 2. TDES (Triple-DES 192)	RNG (it is only generated once, the first time a DKE client needs it, since all clients use same broadcast key)	Encrypted (using Dynamic unicast key)	Plaintext in RAM	Zeroized when local antennae Approved encrypting mode either reconfigured or changed from 3eTI DKE mode to any other local antennae Approved encrypting mode, to bypass mode.	Used to encrypt broadcast and multicast traffic in support of DKE. The same key is used for all DKE clients.
IEEE 802.11i Protocol PSK Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
PSK mode passphrase	ASCII string	Input encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when local antennae Approved encrypting mode either reconfigured or changed from IEEE	Used to derive 802.11i PMK

					802.11i mode to any other local antennae Approved encrypting mode (including 802.11i EAP-TLS), to bypass mode. Zeroized when reset to factory settings.	

IEEE 802.11i Protocol EAP-TLS Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
See EAP-TLS keys/CSPs	-	-	-	-	-	There are 802.11i EAP-TLS-specific EAP-TLS keys/CSPs used to authenticate User operator to module

IEEE 802.11i Protocol Keys/CSPs (Common to PSK and EAP-TLS)						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
PMK	If 802.11i PSK, then derived from PSK mode passphrase: HMAC-SHA1 where passphrase is HMAC key and SSID is hashed. If 802.11i EAP-TLS, then secret key (TLS master secret)	If 802.11i PSK, then ASCII string is input encrypted (using TLS session key) If 802.11i EAP-TLS, then not input, instead derived (TLS master secret resulting from successful User EAP-TLS authentication in DKE mode)	Not output	If 802.11i PSK, then plaintext in flash For both 802.11i PSK and EAP-TLS, plaintext in RAM	Zeroized when local antennae Approved encrypting mode either reconfigured or changed from IEEE 802.11i mode to any other local antennae Approved encrypting mode (including from 802.11i PSK to 802.11i EAP-TLS, and 802.11i EAP-TLS to 802.11i PSK), to bypass mode. If 802.11i PSK, zeroized when reset to factory	802.11i PMK

					settings.	
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 local antennae Approved encrypting mode either reconfigured or changed from IEEE 802.11i mode to any other local antennae Approved encrypting mode (including from 802.11i PSK to 802.11i EAP-TLS, and 802.11i EAP-TLS to 802.11i PSK), to bypass mode. 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 local antennae Approved encrypting mode either reconfigured or changed from IEEE 802.11i mode to any other local antennae Approved encrypting mode	802.11i GTK

					(including from 802.11i PSK to 802.11i EAP-TLS, and 802.11i EAP-TLS to 802.11i PSK), to bypass mode. When re-key period expires	
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	Plaintext in flash	Zeroized when local antennae Approved encrypting mode either reconfigured or changed from 3eTI DKE or IEEE 802.11i EAP-TLS mode to any other local antennae Approved encrypting mode (including to 802.11i PSK), to bypass mode Zeroized when reset to factory settings.	Authenticate module to Security Server in support of DKE and 802.11i EAP-TLS authentication
Backend password	HMAC key (ASCII string)	Input encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when local antennae Approved encrypting mode either reconfigured or changed from 3eTI DKE or IEEE 802.11i EAP-TLS mode to any other local antennae Approved encrypting mode (including to	Authenticate messages between module and security server in support of 802.11i EAP-TLS

					802.11i PSK), to bypass mode Zeroized when reset to factory settings.	
Backend key	AES ECB key (d;128)	Input encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when local antennae Approved encrypting mode either reconfigured or changed from 3eTI DKE or IEEE 802.11i EAP-TLS mode to any other local antennae Approved encrypting mode (including to 802.11i PSK), to bypass mode Zeroized when reset to factory settings.	Decrypt TLS master secret returned to module by Security Server after successful User authentication in support of 802.11i EAP-TLS
DH private exponent	Private DH key	RNG	Not output	Plaintext in RAM	Zeroized after decrypt TLS master secret returned from Security Server Zeroized if the DKE session times out.	Used in DH exchange performed after successful User EAP-TLS authentication in DKE mode
DH session key (a.k.a. AES post authentication key)	AES ECB key (d;128)	Not input (derived from DH exchange)	Not output	Plaintext in RAM	Zeroized when successfully authenticate 3eTI DKE client after decrypt TLS master secret returned from Security Server.	Decrypt TLS master secret returned to module by Security Server after successful User authentication in support of DKE 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) TDES (Triple-DES 192)	Input encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when bridge antenna Approved encrypting mode either reconfigured or when changed from 3eTI bridging mode to any other bridging antenna mode. Zeroized when reset to factory settings.	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 (1024) (key wrapping; key establishment methodology provides 80-bits of encryption strength)	Not input (installed at factory)	Not output	Plaintext in flash	Zeroized during firmware upgrade by overwriting with new firmware image	Used to support CO and Admin HTTPS interfaces.
TLS session key for encryption	Triple-DES (192)	Not input (derived)	Not output	Plaintext in RAM	Zeroized when a page of the web GUI is served after it is used.	TLS server write key

3.6. Self-Tests

The module performs the following self-tests:

Power-up self-tests:

- 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
- DH pairwise consistency test (critical function)
- SHA-1 Integrity Test for firmware

Conditional self-tests:

- CRNGT for Approved PRNG
- CRNGT for non-Approved PRNG (Open SSL based RNG)
- Bypass Tests
- Firmware Load Test using HMAC-SHA-1

3.7. Secure Operation of the AirGuard Wireless Access Point

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

Secure installation, configuration, and operation procedures are below.

3.7.1. Applying Tamper-Evident Seals (All Models)

The following section contains detailed instructions to the Crypto Officer concerning where and how to apply the tamper evident seals to the module enclosure, in order to provide physical security for FIPS 140-2 level 2 requirements. Note the physical security rules are the same between the 525A-3 and the 525A-3MP.

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. ½” length 440 Pan Head screws are used on each circular connector to secure them to the panel. Two 440 KEPS nuts and a nylon washer are added to the inside shaft and tightened together with washers facing each other approximately 1/32” from the

connector panel. This prevents the screws from being removed and thus entry cannot be accomplished without removing the security labels.

Materials:

525A-3 module – 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 the module the placement locations of tamper-evident tape seals. (4 locations as shown in the figures below for the module).
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 module as shown in the figure below. 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 module, apply pressure to verify that adequate adhesion has taken place.

Removal – Tamper-evident tape

1. Locate on the module locations of tamper-evident tape seals. (4 locations (two on each panel) as shown in the figure below for the module)
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 module to allow opening of enclosure.
4. Using 3M adhesive remover or equivalent, remove residual tamper-evident seal tape. (two locations as shown in the figure belowfor the module)

The photos below show the physical interface of the 3e-525A-3 enclosure with tamper evident seals.

3e-525A-3 Side One – Upper Left

3e-525A-3 Side One – Lower Right

3e-525A-3 Side Two

The photos below show the physical interface of the 3e-525A-3 BASIC enclosure with tamper evident seals.

3e-525A-3 BASIC Side One

3e-525A-3 BASIC Side Two

The photos below show the physical interface of the 3e-525A-3MP enclosure with tamper evident seals.

3e-525A-3MP Side One

3e-525A-3MP Side Two

3.7.2. Checking for Tamper Evidence

Tamper-evident seals should be checked for letters from the word “OPENED” left behind by seal residue when the seal is removed.

Tamper-evident seals should also be checked for nicks and scratches that make the metal case visible through the nicked or scratched seal.

Glossary

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