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

3e-945
AirGuard iMesh Wireless Gateway Cryptographic Module

HW Versions 1.0
FW Versions 1.0

Security Policy
Version 1.1

Revision History

Date	Document Version	Description	Author(s)
10-June-2014	1.0	For External Release	Chris Guo
October-06-2014	1.1		Chris Guo

Table of Contents

1. Introduction

1.1. Purpose

This document describes the non-proprietary cryptographic module security policy for 3e Technologies International's ISA 100.11a wireless gateway product, the *3e-945 AirGuard iMesh Wireless Gateway Cryptographic Module* (Hardware Versions: HW V1.0, Firmware Versions: 1.0). This policy was created to satisfy the requirements of FIPS 140-2 Level 2. It defines 3eTI's security policy and explains how the *3e-945 AireGuard iMesh Wireless Gateway Cryptographic Module* meets the FIPS 140-2 security requirements.

Figure 1 – 3e-945 AirGuard iMesh Wireless Gateway Cryptographic Module

1.2. Cryptographic Module Definition

The *3e-945 AirGuard iMesh Wireless Gateway Cryptographic Module* is a device which consists of electronic hardware, embedded firmware and an enclosure. For purposes of FIPS 140-2, the module is considered to be a multi-chip embedded module. The *3e-945 AirGuard iMesh Wireless Gateway Cryptographic Module* is enclosed in a tamper-resistant opaque metal enclosure, protected by tamper-evident tape intended to provide physical security shown in figure 1. The module's cryptographic boundary is the metal enclosure. The components attached to the underside of the PCB and the components (RTC, reset delay chip, logic gates, and resistors, underside of chip pads, impedance beads and capacitors) which reside outside of the protective "can" of the module are outside the cryptographic boundary and non-security relevant. The table below lists the security level of this module.

Table 1 – Module Security Level

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC11	2
9	Self-tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

1.3. Ports and Interfaces

The module provides one wireless radio, two Ethernet ports and power input as shown in the figure below:

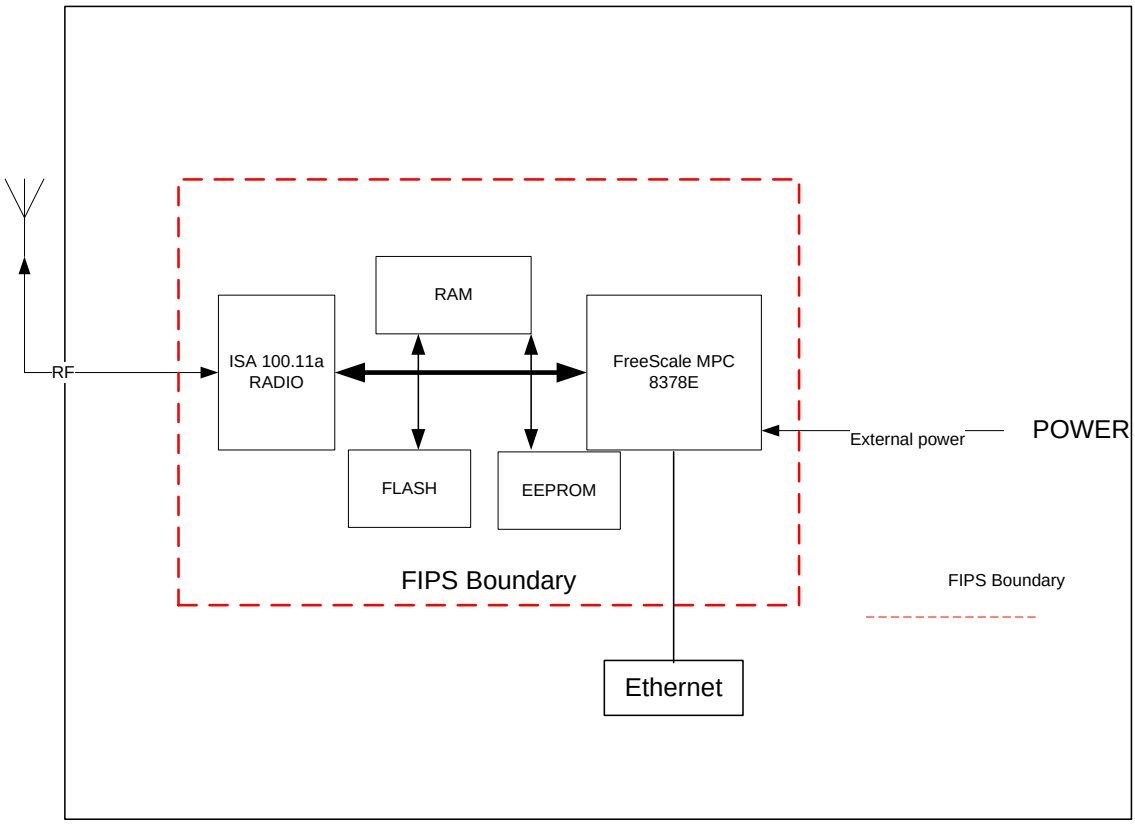


Figure 2 – 3e-945 Wireless Gateway Cryptographic Module High Level Block Diagram

The ports are defined below:

a. Status output: Ethernet ports
b. Data output: Radio interface and Ethernet ports
c. Data input: Radio interface and Ethernet ports
d. Control input: Ethernet ports
e. Power port: External power interface

1.4. Scope

This document covers the secure operation of the *3e-945 AirGuard iMesh Wireless Gateway Cryptographic Module*, including the initialization, roles and responsibilities of operating the product in a secure, FIPS-compliant manner, and a description of the Security Relevant Data Items (SRDIs).

2. Roles, Services, and Authentication

The product firmware supports two separate roles. The set of services available to each role is defined in this section. The product authenticates an operator's role by verifying his/her password or possession of a shared secret.

2.1 Roles & Services

The product supports the following authorized roles for operators:

Crypto Officer Role: The Crypto officer (CO) role performs all security functions provided by the product. This role performs cryptographic initialization and management functions (e.g., module initialization, input/output of cryptographic keys and SRDIs, audit functions and Administrator user management). The Crypto Officer authenticates to the product using a username and password (8-32 characters).

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

- Other ISA 100.11a wireless sensor

The Device Role has access to the data encryption and decryption service (AES-CCM). It's equivalent to the User Role defined in FIPS 140-2.

2.2 Authentication Mechanisms and Strength

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

Table 2 – Authentication versus Roles

Role	Type of Authentication	Authentication Data
Crypto Officer	ID-based	Userid and password
Device ISA100.11a wireless sensor	ID-based	The possession of network join key, identifiable with MAC address

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

Table 3 – Strength of Authentication

Authentication Mechanism	Strength of Mechanism
Userid and password	(8-32 chars) Minimum 8 characters => 94^8 = 6.096E15
Static key	128 bits => 2^128 = 3.40E38

The module halts (introduces a delay) for one second (after each unsuccessful authentication attempt by *Crypto Officer*). 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).

As for the wireless device, the IEEE 15.4 network join key is 128 bits, the probability for a random attempt to succeed is $1:2^{128}$. The fastest network connection supported by the module is 256 Kbps. Hence at most ($256 \times 10^3 \times 60 = 1.536x10^7$) 1,536,000bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is less than 1: ($2^{128} / 1.536x10^7$), which is less than 100,000 as required by FIPS 140-2.

2.3 Services

The Crypto Officer can configure the module while Device users can only use the encryption/decryption service of the module. The table below details the roles and available services

Table 4- Services and Roles

Service and Purpose	Details	Crypto Officer	Device
Input of Keys	Network Join key Firmware verification key	X	
Load Web Server Certificate and private key	Change the web server certificate	X	
Change password	Crypto Officer change his own password only	X	
Load Firmware	Upload new firmware to the module	X	
Show system status	View traffic status and systems log excluding security audit log	X	
Reboot		X	
View Audit Log	View security audit logs	X	
Factory default	Delete all configurations, zeorize keys and CSPs, set device back to factory default state	X	
Perform Self Test	Run algorithm KAT	X	
Wireless data encryption & decryption	Cryptographic service available to the Device User		X
Non Approved TLS Service	RSA Key wrapping during the TLS Session with less than 112 bit	X	X

	encryption strength		
Allowed TLS Services	RSA Key wrapping during the TLS Session with 112-128 bit encryption strength	X	X

The table below shows the services and their access rights to the Critical Security Parameters (CSPs)

Table 5- CSPs and Access by Services

Service and Purpose	CSPs	Access
Input of Keys	Network Join key Firmware verification key	Write
Change password	Crypto Officer password	Read and Write
Show system status	None	None
Load Web Server Certificate and private key	Change the web server certificate	Read and Write
Reboot	All	Write
Factory default	Delete all configurations and set device back to factory default state	Write
Gateway setting and other general configuration	None	None
Wireless data encryption & decryption	AES_CCM 128 bits key	Execute
Non Approved TLS Service	Web Server private key	Execute
Allowed TLS Service	Web Server private key	Execute

3. Secure Operation and Security Rules

By factory default, the device is put in Non-FIPS mode with NO security setting, and the radio is turned on but the network join key is not configured. The module will be running in FIPS mode after Crypto Officer follows the Security Rules.

In order to operate the product securely, each operator shall be aware of the security rules enforced by the module and shall adhere to the physical security rules and secure operation rules detailed in this section.

3.1. Security Rules

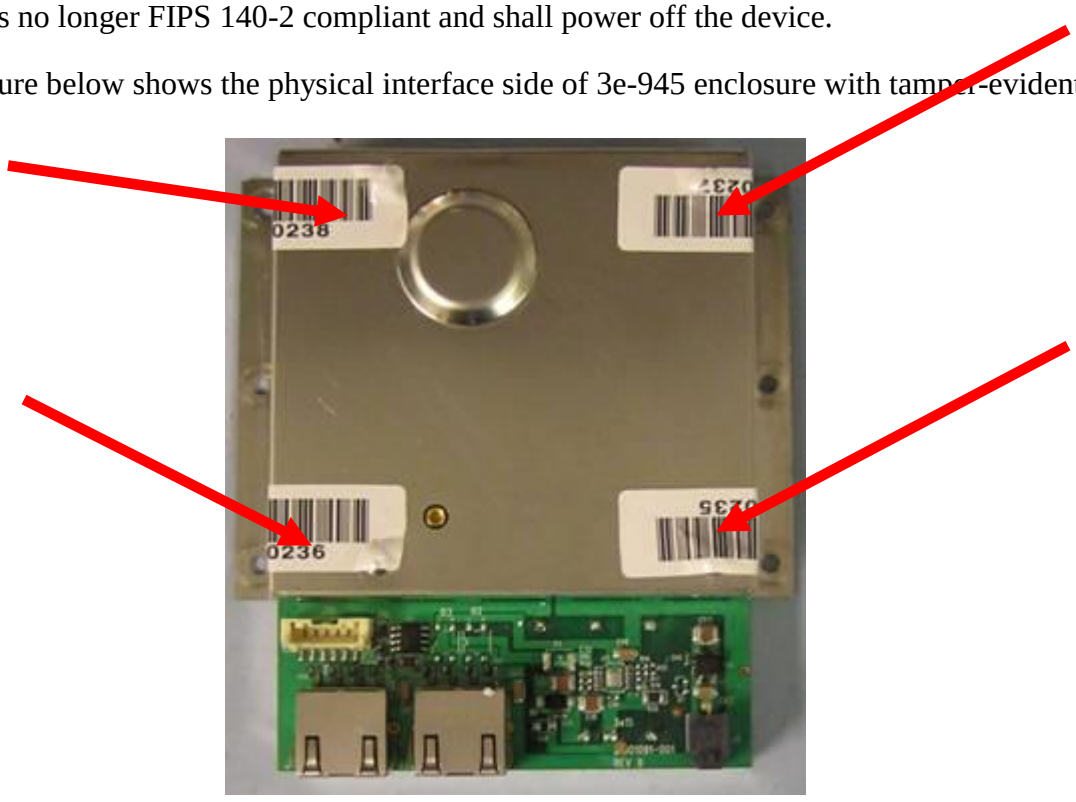
The following product security rules must be followed by the operator in order to ensure secure operation:

1. The Crypto Officer shall not share any key, or SRDI used by the product with any other operator or entity.
2. The Crypto Officer is responsible for inspecting the tamper evident seals. Other signs of tamper include wrinkles, tears and marks on or around the label.
3. The Crypto Officer shall change the default password when configuring the product for the first time or after the device factory default. The default password shall not be used. The module firmware also enforces the password change upon Crypto Officer's first log in.
4. The Crypto Officer shall login to make sure network join key and configured and applied in the device.
5. The Crypto Officer shall load the 2048 or 3072 bits RSA certificate for the device web server.

3.2. Physical Security Tamper Evidence

The physical security provided is intended to meet FIPS 140-2 Level 2 physical security (i.e. tamper evidence). Four tamper evidence tapes are applied at the factory. Crypto Officer should check the integrity of the tape at the first time using the crypto module and later at a yearly interval. In case he/she notices any damage or missing seals, the Crypto Officer shall treat the device as no longer FIPS 140-2 compliant and shall power off the device.

The picture below shows the physical interface side of 3e-945 enclosure with tamper-evident seals.



4. Operational Environment

The crypto module firmware runs on FreeScale PowQUICC 8378E processor. The firmware is embedded within and it is non-modifiable. In that an operator cannot reconfigure the internal firmware to add/delete/modify functionality. 3eTI allows a single case in which firmware can ever be modified: an upload image can be loaded if a bug is found or an enhancement to the 3e-945 needs to be added. The current version of the firmware is 1.0.

5. Security Relevant Data Items

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

5.1. Cryptographic Algorithms

The product supports the following FIPS-approved cryptographic algorithms. The algorithms are listed below, along with their corresponding CAVP certificate numbers.

3e Technologies International Inc. 3eTI OpenSSL Algorithm Implementation 1.0.1-a	
Triple-DES:	#1327
AES:	#2060
SHS:	#1801
RSA:	#1491
ECDSA verify with P256 curve	#303
RNG:	#1076
Component Test (TLS 1.0/1.1/1.2 with SHA-256/SHA-384)	#285

NIVIS Radio Hardware Encryption Engine	
AES (CCM, CMAC)	#1611

The product supports the following non-Approved but allowed cryptographic algorithms:

- MD5
- NDRNG
- RSA (key wrapping; key establishment methodology provides 112-128 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- 3-key Triple-DES (Cert. #1327, key wrapping; key establishment methodology provides 112 bits of encryption strength)
- AES (Cert. #2060, key wrapping; key establishment methodology provides between 128 – 256 bits of encryption strength)

5.2. Self-tests

POST (Power on Self Tests) is performed on each boot. A command to reboot the device is considered on-demand self test. The Crypto Officer has access to the web GUI to initiate the reboot/self test.

5.2.1 Power-on Self-tests

3eTI 945 Wireless Gateway Cryptographic Module Power-on self-tests include all known answers test for algorithms listed above.

- AES ECB 128/192/256 bit – encrypt KAT
- AES ECB 128/192/256 bit – decrypt KAT
- Triple-DES CBC –3 keys encrypt KAT
- Triple-DES CBC –3 keys decrypt KAT
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
- RSA SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 sign KAT
- RSA SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 verify KAT
- ANSI X9.31 RNG KAT
- TLS 1.0/1.1 and 1.2 KDF with SHA256/SHA384 KAT

**ECDSA verification is supported by the module. There is no separate test for it since the integrity test meets the requirement.*

NIVIS Radio Hardware Encryption Engine Power-on self-tests:

- AES CCM 128 bit - encrypt KAT
- AES CCM 128 bit - decrypt KAT

Firmware Integrity Test

- Firmware Integrity Test with ECDSA P256 curve verify
- File System Integrity Test with ECDSA P256 curve verify, this guarantees the radio firmware integrity before it's loaded into the radio.

Firmware integrity is performed at POST (Power On Self Test) during module boot up.

5.2.2 Conditional Self-tests

- Continuous Random Number Generator Test (CRNGT) on Approved RNG
- Continuous Number Generator Test (CRNGT) on NDRNG
- Firmware load test

5.3. Cryptographic Keys and SRDIs

The module contains the following security relevant data items:

Table 6 - SRDIs

Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
Operator passwords	ASCII string	Input over HTTPS WEB GUI	Not output	PKCS5 format is stored in Flash	Zeroized when reset to factory settings.	Used to authenticate CryptoOfficer
Firmware verification key	ECDSA 256 bits public key	Embedded in firmware at compile time.	Not output	Plaintext in flash	N/A	Used for firmware digital signature verification
AES_CCM key	Encryption key used in ISA100.11a traffic	Input through HTTPS WEB GUI	Output to peer device via AES key wrap	Plaintext in RAM	Zeorized when connection drop	Use to encrypt/decrypt the wireless traffic data
ISA 100.11a radio network join key	AES key (HEX string)	Updated value through HTTPS WEB GUI	Not output	Plaintext in FLASH Plaintext in Radio FLASH storage	Zeroized when firmware is upgraded or new value is input through local management console.	Used to authenticate peer device and encrypt radio session key with AES_CCM
ISA 100.11a radio session key	AES Key, 128 bits	Not input, generated by the module using approved RNG	Output to peer device, encrypted with radio network join key	Plain text in RAM	Zeorized with session closes.	Use to encrypt/decrypt ISA 100 wireless data
FIPS ANSI X9.31RNG Seed Key	16/32-byte value	128/256 bits read from /dev/random	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 RNG
RNG Seed	16 byte value	128 bits read from /dev/random	Not output	Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS PRNG after it is used.	Used as seed for FIPS RNG.
RSA private key	RSA (2048/3072) (key wrapping; key	Loadable by Crypto Officer via HTTPS Web	Not output	Plaintext in flash	Zeroized when new server certificate/pri	Used to support CO HTTPS interfaces.

	establishment methodology provides 112-128 bits of encryption strength)	GUI			vate key is uploaded.	
TLS session key for encryption	Triple-DES (192) AES (128/192/256)	Not input, derived using TLS protocol	Not output	Plaintext in RAM	Zeroized when HTTPs session terminates	Used to protect HTTPS session.
Certificate Authority (CA) public key certificate	"CA public key"	Not input (installed at factory)	Not output	Plaintext in flash	N/A	Used in HTTPS session
TLS Server Certificate	Server public key	Loadable by Crypto Officer via HTTPS Web GUI	Plaintext in Flash	Plaintext in flash	N/A	Used in HTTPS session

6. Design Assurance

All source code and design documentation for this module are stored in version control system CVS. The module is coded in C with module's components directly corresponding to the security policy's rules of operation. Functional Specification is also provided.