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

3e-543
AirGuard iField Wireless Sensor Cryptographic Module

HW Versions 1.0
FW Versions 1.0

Security Policy
Version 1.0

January 2014

GLOSSARY OF TERMS 3

1. INTRODUCTION 4

1.1. PURPOSE 4
1.2. DEFINITION 4
1.3. PORTS AND INTERFACES 5
1.4. SCOPE 6

2. ROLES, SERVICES, AND AUTHENTICATION 6

2.1 ROLES & SERVICES 7
2.2 AUTHENTICATION MECHANISMS AND STRENGTH 7
2.3 SERVICES 8

3. SECURE OPERATION AND SECURITY RULES 10

3.1. SECURITY RULES 10
3.2. PHYSICAL SECURITY TAMPER EVIDENCE 10

4. OPERATIONAL ENVIRONMENT 12

5. SECURITY RELEVANT DATA ITEMS 12

5.1. CRYPTOGRAPHIC ALGORITHMS 12
5.2. SELF-TESTS 12
5.2.1 Power-on Self-tests 12
5.3 CRYPTOGRAPHIC KEYS AND SRDIS 13

6. DESIGN ASSURANCE 14

Glossary of terms

CO	Cryptographic Officer
FIPS	Federal Information Processing Standard
MAC	Medium Access Control
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SRDI	Security Relevant Data Item
ISA	International Society of Automation

1. Introduction

1.1. Purpose

This document describes the non-proprietary cryptographic module security policy for 3e Technologies International's ISA 100.11a wireless sensor product, the *3e-543 AirGuard iField Wireless Sensor 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-543 AireGuard iField Wireless Sensor Cryptographic Module* meets the FIPS 140-2 security requirements.

The figure below shows the *3e-543 Secure Access Point Cryptographic Module*.

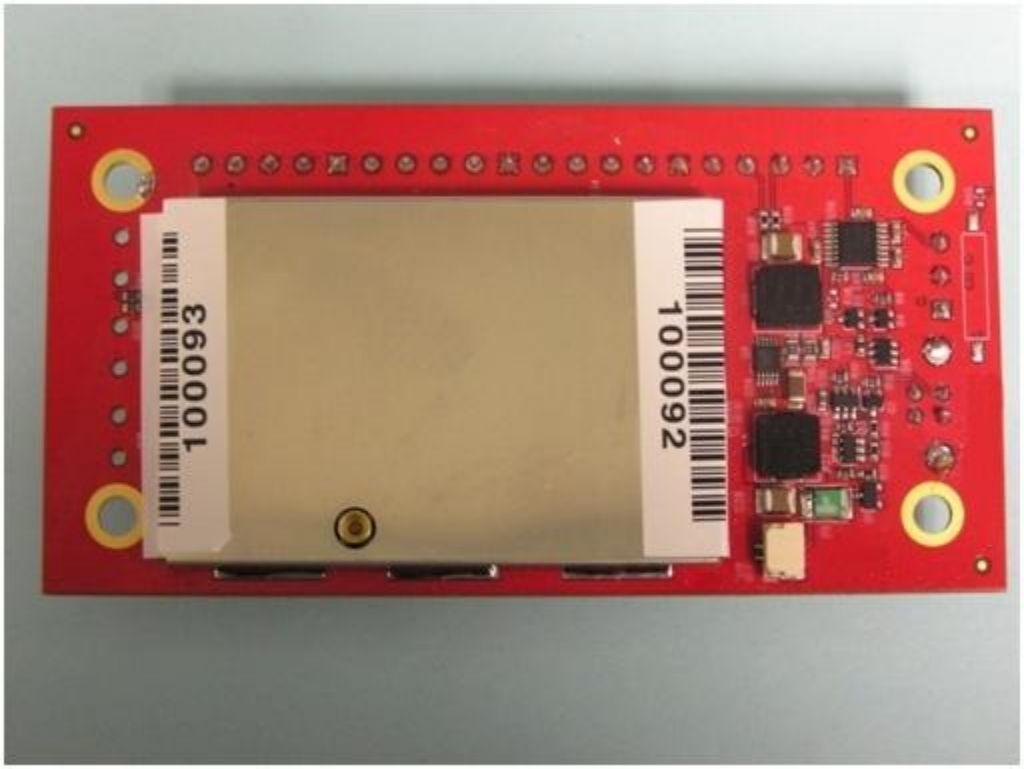


Figure 1 – 3e-543 AirGuard iField Wireless Sensor Cryptographic Module

1.2. Definition

The *3e-543 AirGuard iField Wireless Sensor Cryptographic Module* is a device which consists of electronic hardware, embedded software and an enclosure. For purposes of FIPS 140-2, the module is considered to be a multi-chip embedded module. The *3e-543 AirGuard iField Wireless Sensor 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 excluded from FIPS requirements. This device always runs in FIPS mode. 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	2
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
14	Cryptographic Module Security Policy	2

1.3. Ports and Interfaces

The module provides sensor analog and digital connection pins, one wireless radio, LEDs and USB port for serial management session communication and power input as shown in the figure below:

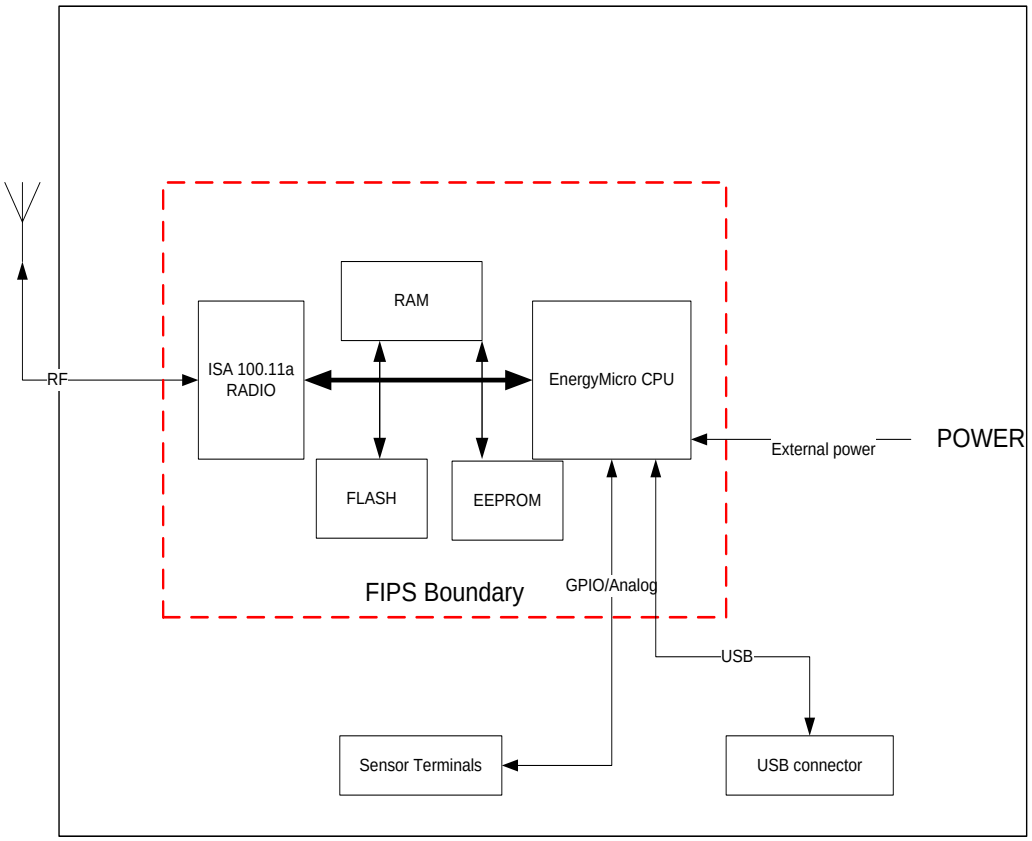


Figure 2 – 3e-543 Wireless Sensor Cryptographic Module High Level Block Diagram

The ports are defined below:

a. Status output: USB port and LED (GPIO) pins
b. Data output: Radio interface
c. Data input: Radio interface, USB port and sensor terminal pins
d. Control input: USB port, radio interface and reset pin
e. Power port

1.4. Scope

This document covers the secure operation of the *3e-543 AirGuard iField Wireless Sensor 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 software supports three 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).

Administrator User Role: This role performs general product configuration. No CO security functions are available to the Administrator. The Administrator can also reboot the product if deemed necessary. The Administrator 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
- ISA 100.11a wireless gateway

The Device Role has access to the data encryption and decryption service (AES-CCM). The is the only FIPS 140-2 corresponding "User" role.

NetUser Role: This is a special administrator role assumed by the ISA100 Gateway device when the Gateway loads firmware into the module using the encrypted wireless data link. The NetUser authenticates to the module with user name and password. The only extra service available to this role is to load firmware over wireless link.

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 Administrator User NetUser	ID-based	Userid and password
Device ISA100.11a wireless sensor	Static key	The possession of network join key, identifiable with MAC address
ISA 100.11a wireless gateway	Static key	The possession of the 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 (initial value and keep incrementing) after each unsuccessful authentication attempt by *Crypto Officer* or *Administrator*. 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 ($256 \times 10^3 \times 60 = 1.536 \times 10^7$) 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: ($2^{128} / 1.536 \times 10^7$), which is less than 100,000 as required by FIPS 140-2.

2.3 Services

The Crypto Officer and Administrator 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	Administrator	Device	NetUser
Input of Keys	Network Join key Firmware verification key	X			
Create and manage Administrator user	Support up to 10 administrator users	X			
Change password	Administrator change his own password only	X	X		
Load Firmware	Upload new firmware to the	X			X

	module				
Show system status	View traffic status and systems log excluding security audit log	X	X		
Key zeroization via reboot		X	X		
View Audit Log	View security audit logs	X			
Factory default	Delete all configurations and set device back to factory default state	X	X		
Sensor setting and other general configuration		X	X		
Wireless data encryption & decryption				X	X

Please note that the Crypto Officer should only load the NIST FIPS validated firmware as indicated in this document. Loading invalidated firmware will result in the module operating in non-validated mode.

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
Create and manage Administrator user	Administrator Password	Read and Write
Change password	CryptoOfficer, Administrator or NetUser password	Read and Write
Show system status	None	None
Key zeroization via reboot	All	Write
Factory default	Delete all configurations and set device back to factory default state	Write
Sensor setting and other general configuration	None	None
Wireless data encryption & decryption		Execute

3. Secure Operation and Security Rules

By factory default, the device is put in FIPS mode with NO security setting, and the radio is turned on but the network join key is not configured.

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:

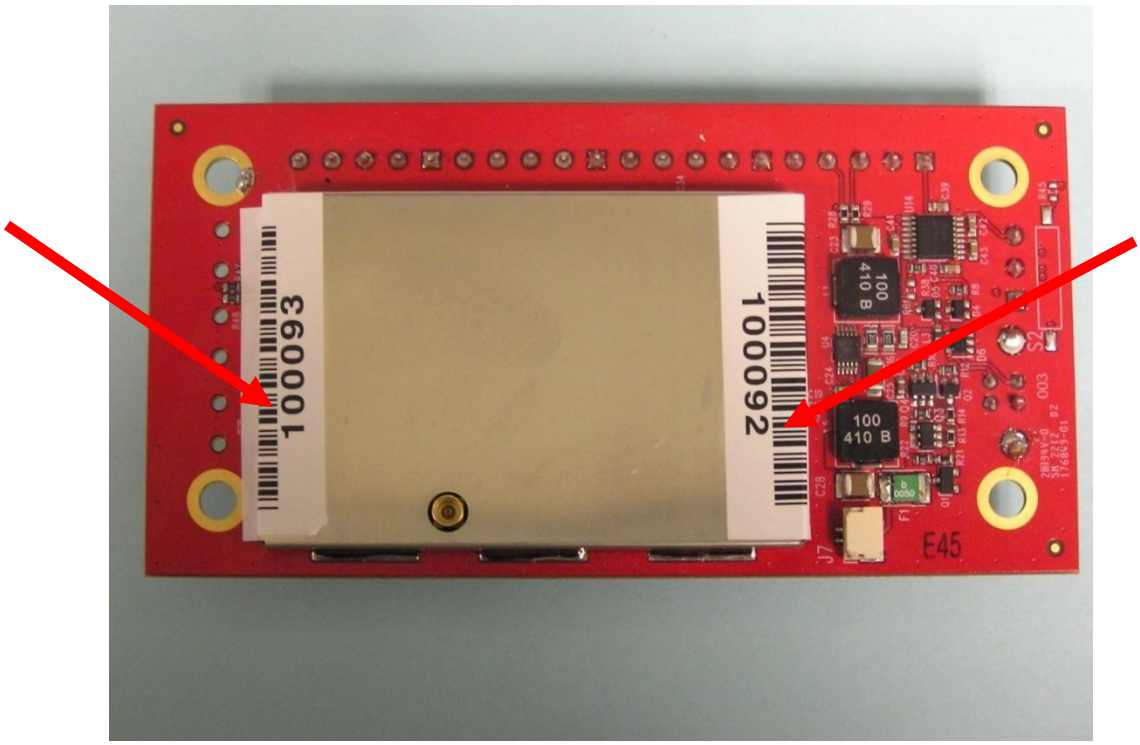
1. The Crypto Officer shall not share any key, or SRDI used by the product with any other operator or entity.
2. The Crypto officer is responsible for inspecting the tamper evident seals. Other signs of tamper include wrinkles, tears and marks on or around the label.
3. The Crypto Officer shall change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

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). The tamper evidence tape is applied at the factory. Crypto Officer should check the integrity of the tape at the first time using the crypto module and later at one year interval. In case he/she notices any damage or missing seals, the Crypto Officer shall treat the device no longer in FIPS mode of operation and shall power off the device.

The picture below shows the physical interface side of 3e-543 enclosure with tamper-evident seals.

Figure 3 – 3e-543 with tamper seals


100093
100092
100
410 B
100
410 B
E45

4. Operational Environment

This module uses Energy Micro EFM32 processor with 3eTI embedded firmware. The firmware version 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. Sensor Cryptographic Library Algorithm Implementation version 1.0

AES:	#2251
SHS: SHA-1, SHA-256	#1939
HMAC: SHA-1, SHA-256	#1379
ECDSA verify with P256 curve	#359

NIVIS Radio Hardware Encryption Engine

AES (CCM, CMAC)	#1611

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 "Crypto Officer" can send reboot command from serial console GUI.

5.2.1 Power-on Self-tests

3eTI 543 Sensor Cryptographic Module Power-on self-tests include all known answers test for algorithms listed above.

- AES CCM 128 – encrypt KAT
- AES CCM 128 – decrypt KAT
- SHA-1, SHA-256 KAT
- HMAC-SHA-1, HMAC-SHA-256 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

Software Integrity Test

- Firmware Integrity Test with ECDSA P256 curve verify
- Radio firmware Integrity Test with ECDSA P256 curve verify

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

5.2.2 Conditional Self-tests

Whenever a firmware package (for the application processor) is uploaded through GUI console over USB port or over the air, the package integrity check is performed before the firmware can be updated. The firmware package is digitally signed with 3eTI ECDSA private key and the crypto module performs ECDSA verify before accepting the firmware.

Whenever a radio firmware is uploaded either through the GUI console or Over the Air (OTA), the radio firmware's integrity is checked via ECDSA before acceptance. Then the radio is rebooted with the newly updated firmware and all self tests are performed again.

Whenever a key is input through the local USB console, double entries are required the two entries are compare to make sure the contents are identical. In case of inconsistent key entries, the key input will be rejected.

5.3 Cryptographic Keys and SRDIs

The module contains the following security relevant data items:

Table 6 - SRDIs

Keys/CSPs						
Key/CSP	**Type**	**Generation/**	**Output**	**Storage**	**Zeroization**	**Use**

		Input				
Operator passwords	ASCII string	Input over serial console	Not output	Hashed value is stored in EEPROM	Zeroized when reset to factory settings.	Used to authenticate CryptoOfficer Or Administrator User
Firmware verification key	ECDSA public key	Embedded in firmware at compile time. One additional key can be input through serial console	Not output	Plaintext in flash	N/A	Used for firmware digital signature verification
ISA 100.11a radio network join key	AES key (HEX string)	Updated value through serial console and stored in EEPROM	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 communicate with ISA 100.11a Gateway and data packets encryption/decryption (AES_CCM)
HMAC Key	ASCII string 4-64 chars	Input over serial console	Not output	Plaintext in flash	Zeroized when reset to factory settings or changed via console	Message authentication
Application Data Encryption Key	AES_CCM Key (HEX string)	Input over serial console	No output	Plaintext in flash	Zeroized when new values is input or at factory default	Used to encrypt the application level data

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.