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

3e-636M-HSE CyberFence Cryptographic Module

HW Version (1.0)
FW Version (5.0)

Security Policy Version 1.6

May 2016

Copyright ©2016 by 3e Technologies International.
This document may freely be reproduced and distributed in its entirety.

Revision History

Date	Document Version	Description	Author(s)
10-June-2014	1.0	For External Release	Chris Guo
September-15-2014	1.1	Updated after Cygnacom review	Chris Guo
September-19-2014	1.2	Updated for release to CMVP	Chris Guo
February-23-2015	1.3	Updated after NIST review	Chris Guo
January-12-2016	1.4	Updated DRBG	Chris Guo
March-17-2016	1.5	Updated for release to CMVP	Chris Guo
May-13-2016	1.6	Updated for release to CMVP	Chris Guo

Table of Contents

1. Introduction 1
1.1 Cryptographic Module Definition 1
1.2 Cryptographic Module Validation 2
2. Ports & Interfaces 2
3. Roles & services 3
3.1 End User role 4
3.2 Crypto Officer and Administrator Roles 4
4. Operational Environment 7
5. Cryptographic Algorithms 7
6. Cryptographic Keys and SRDIs 8
7. Self-Tests 10
8. Tamper Evidence 11
9. Secure Rules & Configuration 12
10. Design Assurance 12
11. Mitigation of Other Attack 12

1. Introduction

This is a non-proprietary Cryptographic Module Security Policy for the 3e-636M-HSE CyberFence Cryptographic Module from 3e Technologies International. This Security Policy describes how the 3e-636M-HSE meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules.

1.1 Cryptographic Module Definition

The 3e-636M-HSE Crypto Module primarily acts as an inline encryption device. Using AES encryption, it secures IEEE 802.3 MAC layer data between nodes in a local area network or across multiple Virtual Local Area Networks (VLANs). Furthermore, it employs firewall and packet inspection to provide defense-in-depth capabilities to prevent malicious attacks.

The crypto module includes one FreeScale PowQUICC 8378E processor as a multi-function host processor, network processor, and cryptographic processor. The cryptographic module consists of electronic hardware, embedded firmware and enclosure. It is a multiple-chip embedded module for the purposes of FIPS 140-2.

Figure 1 below shows the picture of the 3e-636M-HSE Crypto Module:

Figure 1 – 3e-636M-HSE Crypto Module

The critical circuits of the 3e-636M-HSE Crypto Module are enclosed in a tamper-resistant opaque metal enclosure, protected by tamper evidence tape intended to provide physical security. 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) are outside the cryptographic boundary and non-security relevant.

1.2 Cryptographic Module Validation

The module is validated at the FIPS 140-2 Section levels listed in Table 1 below. The overall security level of the module is 2.

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

Table 1: Module Security Level

2. Ports & Interfaces

The 3e-636M-HSE Crypto Module contains a simple set of interfaces, as shown in the Figure 2 below:

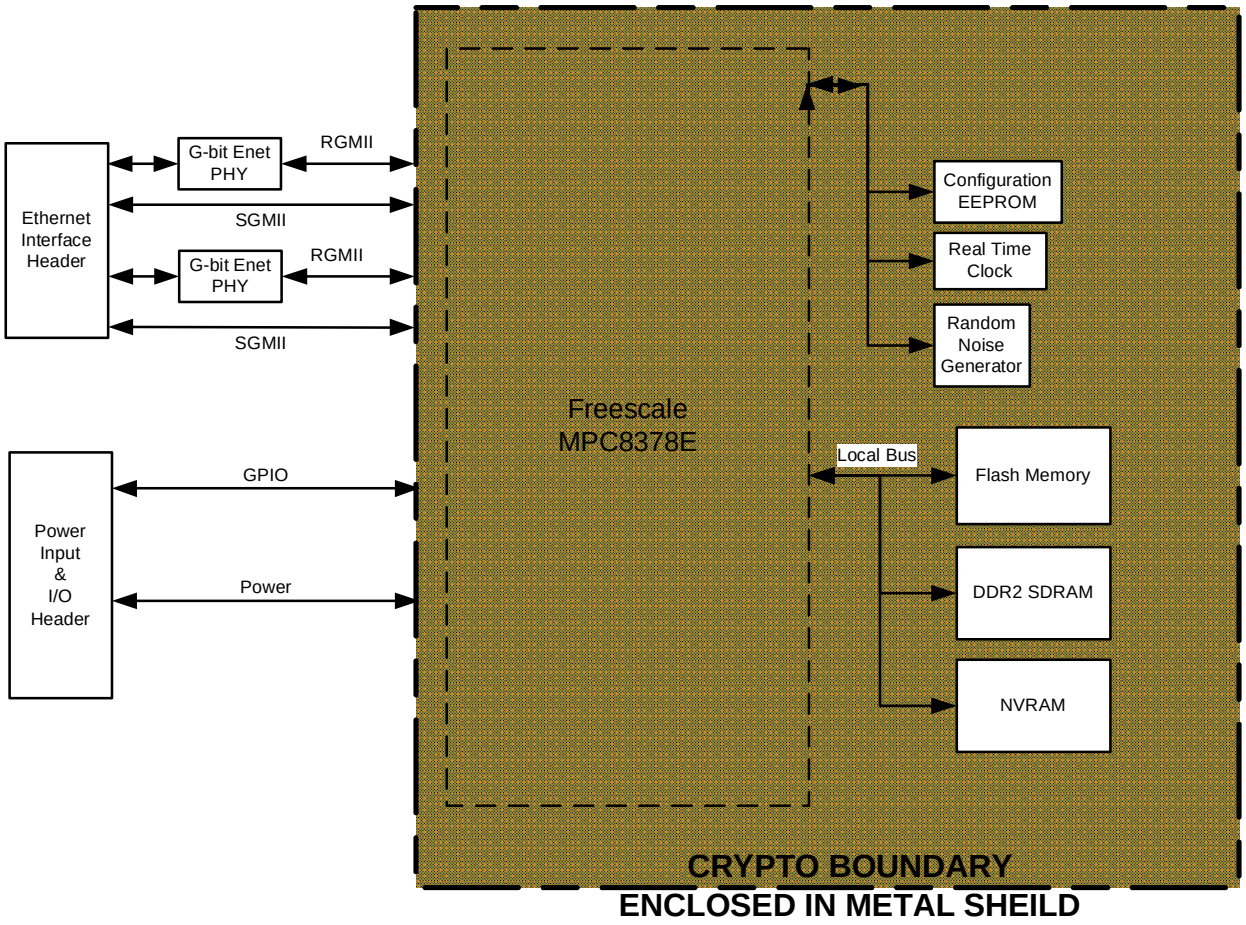

Figure 2 – 3e-636M-HSE Crypto Module High Level Block Diagram

The logical ports:

a. Status output: Ethernet port pins and GPIO (LED) connector pins
b. Data output: Ethernet port pins
c. Data input: Ethernet port pins
d. Control input: Ethernet port pins
e. Power input pin

3. Roles & services

The module supports three separate roles. There are two operator roles and one end user role. The set of services available to each role is defined in this section.

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

Role	Authentication Mechanism	Strength of Mechanism
Crypto Officer	Identity-based , Username and password	(8-30 chars) Minimum 8 characters => 1:94^8 = 1.641E-16
Administrator	Identity-based , Username and password	(8-30 chars) Minimum 8 characters => 1:94^8 = 1.641E-16
End User	Role-based, Encryption/Decryption Key	128/192/256 bits key for AES

Table 2: Authentication & Strength of Authentication

The module halts (introduces a delay) for one second 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).

The module does allow the Crypto Officer to configure particular VLAN into bypass mode; in that case, the End User device on that VLAN is not authenticated by the module. The End User does not use any cryptographic services of the module either. Data in plaintext form is passed from one port to another.

3.1 End User role

The end user of the device can send or receive data to and from the module. End user can only use the cryptographic service but can't configure the device. The End User is authenticated via its possession of the symmetric encryption key.

Using conservative estimates, for an end user possessing the 112 bit symmetric key, the probability for a random attempt to succeed is $1:2^{112}$. The fastest network connection supported by the module is 1 Gbps. Hence at most ($1 \times 10^9 \times 60 = 6 \times 10^{10}$) 60,000,000,000 bits of data can be transmitted in one minute. The number of possible attacks per minutes is $6 \times 10^{10}/112$. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is less than 1: (2^{112} x112/ 60×10^9), which is less than 100,000 as required by FIPS 140-2.

When the device is in End User role, authentication of the End User is performed via its possession of the symmetric key. Per packet integrity check can be optionally turned on by using HMAC-SHA1 or AES_CCM.

3.2 Crypto Officer and Administrator Roles

When a Crypto Officer or Administrator logs into the module using a *username* and a *password* through HTTP over TLS secure channel, the device assumes the role of a Crypto Officer or Administrator.

The Crypto Officer is responsible for performing all cryptographic configurations for the module which include loading Web Server certificate and private key, input VLAN encryption keys, setting Firewall and deep package inspection policies, managing Administrator users, uploading

new firmware and bootloader, setting the password policy and performing self-tests on demand, and performing key zeroization. The Administrator user can configure non-security related parameter of the system such as host name and IP address, view status, and reset the module to factory default settings.

The following table describes the 3e-636M-HSE services, including purpose and functions, and the details about the service:

Table 3: Services and User Access

Service and Purpose	Details	Crypto Officer	Administrator	End User
Input of Keys	Per VLAN encryption key, SNMPv3 encryption key, SNMPv3 authentication key	X		
Input Web server certificate and private key	Web server certificate, certificate private key and root certificate	X		
Configure VLAN into bypass mode	Configure a particular VLAN into bypass mode, under which, the end user is not authenticated to the module nor does it use any cryptographic service of the module. The data is passed from one port to another	X		
Create and manage Administrator user	Support up to 5 administrator users	X		
Change administrator password	Administrator change his own password only	X	X	
Change password of Crypto Officer	Crypto Officer change his own password	X		
Show system status	View traffic status , VLAN configurations (VLAN encryption mode or bypass mode) and systems log excluding security audit log	X	X	
Reboot	Zeroize all keys in RAM	X	X	
Factory default	Delete all configurations and set device back to factory default state	X	X	
Perform Self Test	Run algorithm KAT	X	X	
Load New Firmware	Upload 3eTI digital	X		

	signed firmware			
SNMP Management	All SNMP setting including SNMPv3 encryption key, SNMPv3 authentication key	X	X	
VLAN data encryption & decryption	Module performs data encryption/decryption for each End User			X
VLAN Bypass				X

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

Table 4- CSPs and Access by Services

Service and Purpose	**CSPs**	**Access**
Input of Keys	Per VLAN data encryption key, SNMPv3 encryption key, SNMPv3 authentication key	Write
Input Module Web server certificate and private key	Web Server certificate, private key	Read and Write
Configure VLAN into bypass mode	Per VLAN data encryption key	Write (zeroize prior keys)
Create and manage Administrator user	Administrator Password	Read and Write
Change administrator password	Crypto Officer, Administrator	Read and Write
Change password of Crypto Officer	Crypto Officer password	Read and Write
Show system status	None	None
Reboot	All	Write
Factory default	Delete all configurations and set device back to factory default state	Write
Perform Self Test	None	None
Load new firmware	Firmware signing public key	Read
SNMP management	SNMPv3 encryption key SNMPv3 authentication key SNMP Community Name	Read
VLAN data encryption & decryption	Per VLAN data encryption key	Execute
VLAN Bypass	None	N/A

4. Operational Environment

The crypto module firmware runs on FreeScale PowQUICC 8378E processor. The firmware is embedded within and it is limited-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-636M-HSE needs to be added. The current version of the firmware is 5.0. The module uses digital signature to validate the upload firmware. Non-validated firmware will result in invalidated module.

5. 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

AES	#2060
SHS	#1801
RSA	#1491
HMAC	#1253
ECDSA verify with P256	#303
DRBG	#822
CVL (TLS 1.0/1.1/1.2 with SHA-256/SHA-384)	#285

KTS (AES Cert. #2060 and HMAC Cert. #1253; key establishment methodology provides between 128 and 256 bits of encryption strength)

The TLS KDF is CAVP validated, however the TLS protocol is neither reviewed nor tested by CMVP or CAVP.

3e Technologies International Inc. 3e-520 Accelerated Crypto Core 1.0

AES (ECB, CBC, CCM)	#2078
SHS	#1807
HMAC	#1259

The product supports the following non-Approved cryptographic algorithms:

- MD5
- NDRNG
- RSA (key wrapping; key establishment methodology provides 112-128 bits of encryption strength)

- SNMPv3 KDF (non-compliant)

6. Cryptographic Keys and SRDIs

All keys are entered encrypted using **HTTP over TLS** through the Module Web interface. Below is the Cryptographic Key and Security Relevant Data Item (SRDI) table:

Table 5: SRDI Table

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	PKCS5 hash in flash	Zeroized when reset to factory settings.	Used to authenticate CO and Admin role operators
Firmware verification key	ECDSA public key (256 bits)	Embedded in firmware at compile time. Firmware upgrade is through encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when firmware is upgraded.	Used for firmware digital signature verification
SNMPv3 authentication keys	HMAC key (ASCII string, 128-256 bits)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	Zeroized when reset to factory settings.	Use for SNMP message authentication in non-FIPS mode only
SNMPv3 encryption key	128 bits AES key	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	Zeroized when reset to factory settings.	Use for SNMP message encryption in non-FIPS mode only
system config AES key (256 bit)	AES key (HEX string)	Hardcoded in FLASH	Not output	Plaintext in FLASH	Zeroized when firmware is upgraded.	Used to encrypt the configuration file
RNG Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
DRBG CTR V	32-byte value	32 bytes from /dev/ random which is fed by hardware noise generator	Not output	Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS DRBGafter it is used.	Used as V value for AES CTR for FIPS DRBG.

DRBG CTR key	32-byte value	32 bytes from /dev/ random which is fed by hardware noise generator	Not output	Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS DRBGafter it is used.	Used as key for AES CTR for FIPS DRBG.
VLAN Data Encryption						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
VLAN Data Encryption key (one per VLAN, up to 16 VLANs)	128/192/256 bits AES symmetric key	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	Zeroized at factory default reset	Used to encrypt/decrypt data per VLAN
HMAC-SHA1 key	160 bits key	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	Zeroized at factory default reset	Used to generate keyed digest for the encrypted VLAN data, adding integrity for AES ECB or CBC mode.
RFC 2818 HTTPS Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
Web Server private key	RSA (2048/3072) (key wrapping; key establishment methodology provides 112-128 bits of encryption strength)	installed at factory, can be loaded by Crypto Officer. Input encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when new private key is uploaded	Used to support CO and Admin HTTPS interfaces.
TLS session key for encryption	AES (128/192/256)	Not input, derived using TLS protocol	Not output	Plaintext in RAM	Zeroized when a page of the web GUI is served after it is used.	Used to protect HTTPS session.
Public Security Parameter						
Web Server Public certificate	RSA (2048/3072)	installed at factory, can be loaded by Crypto Officer Input encrypted (using TLS session key)	During TLS session setup	Plaintext in flash	Zeroized when new certificate is loaded	Used to setup TLS session for HTTPS
Web Server root certificate	RSA (2048/3072/4096)	installed at factory, can be loaded by Crypto Officer Input	Not output	Plaintext in flash	Zeroized when new root certificate is loaded	Used to setup TLS session for HTTPS

		encrypted (using TLS session key)				

7. Self-Tests

The 3e-636M-HSE Accelerated Crypto Module performs the following power-on self-tests:

Firmware Integrity Test

- Bootloader Integrity Test
- Firmware Integrity Test

FreeScale PowerQUICC Crypto Engine Power-on self-tests:

- AES ECB encrypt KAT
- AES ECB decrypt KAT
- AES CBC encrypt KAT
- AES CBC decrypt KAT
- AES_CCM encrypt KAT
- AES_CCM decrypt KAT
- SHA-1 KAT
- HMAC SHA-1, SHA224, SHA256, SHA384, SHA512 KAT

3eTI OpenSSL library Power-on self-tests:

- AES ECB encrypt KAT
- AES ECB decrypt KAT
- HMAC SHA-1, SHA224, SHA256, SHA384, SHA512 KAT
- SHA-1 KAT
- FIPS SP800-90A DRBG KATs
- RSA sign KAT
- RSA verify KAT

After device is powered on, the first thing done by bootloader is to check its own integrity. If the integrity is broken, firmware won't boot. Firmware integrity is performed at firmware boot up. Both firmware and bootloader are digitally signed with ECDSA. As for firmware upgrade via Web GUI, the firmware's digital signature is verified via ECDSA prior to its acceptance. If the ECDSA verification fails, the firmware upload will be rejected.

Conditional self-tests:

- Continuous Random Number Generator Test (CRNGT) on DRBG
- DRBG Health Tests
- Continuous Number Generator Test (CRNGT) on NDRNG
- Firmware load test
- VLAN bypass test

Upon self-tests or conditional tests failure, the system will halt and the module will not be operable. The status output LED GPIO pins will be set high to indicate the system halt condition.

8. Tamper Evidence

The cryptographic boundary is protected by two self-destructive tamper evidence tapes, as shown in the figure below.

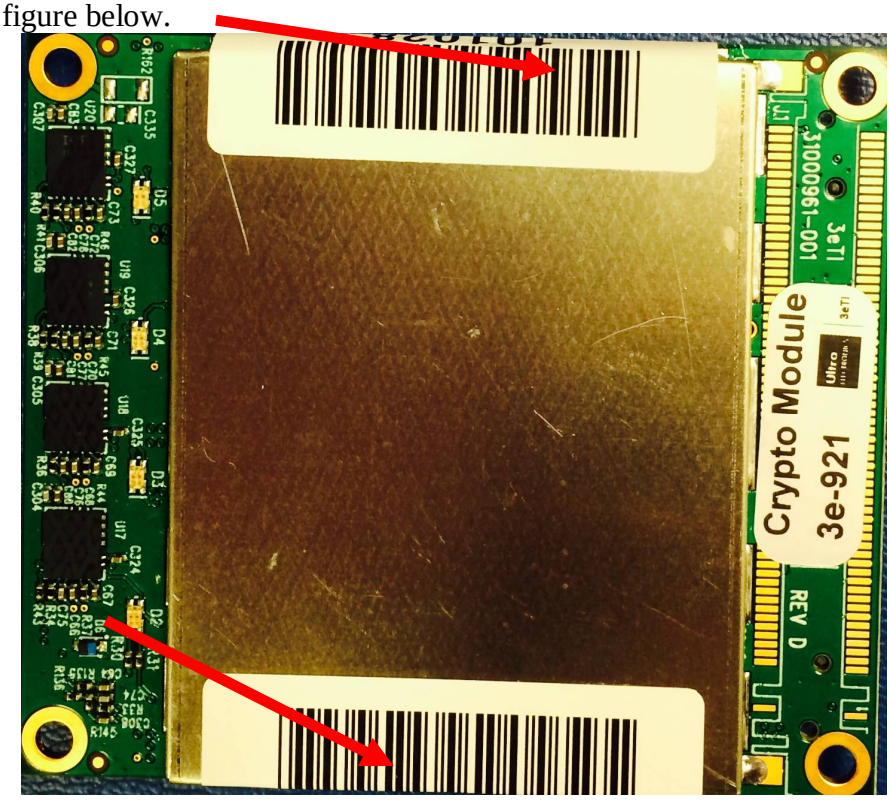

Figure 3 – 3e-636M-HSE Crypto Module Tamper Evidence Tape

Tamper evidence tapes are applied to the module at manufacturing time. Crypto Officer is responsible for checking tamper evidence tapes. It's recommended that Crypto Officer inspect the tamper evidence at every 6 months interval.

Checking for Tamper Evidence

Tamper evidence tapes should be checked for nicks and scratches that make the metal case visible through the nicked or scratched seal.

Tamper evidence tapes may show any of the following as evidence of tampering or removal:

- Tape is not preset in the positions prescribed (as shown above)
- Tape has been cut
- Tape is not stuck down well, or loose
- Self destruction of the tape (broken bits or shreds) present as from an attempt of removal.
- Tracking numbers do not match those recorded

In case of notification of tamper evidence, Crypto Officer shall not power on this module and shall contact 3eTI for factory repair.

9. Secure Rules & Configuration

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 evidence tapes. Other signs of tamper include wrinkles, tears and marks on or around the tape.
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 firmware also enforces the password change upon Crypto Officer's first log in.
4. The Crypto Officer shall login to make sure CSPs and keys are configured and applied in the device.
5. The Crypto Officer shall make sure the key size of the Web server certificate is equal or greater than 2048 bits.
6. The Crypto Officer shall make sure the SNMP is disabled.

Security Configuration

The Crypto Officer shall properly configure the module following the steps listed below:

1. Log in the module over HTTPS and change the default password (If this is the first time of use).
2. Configure the VLAN encryption keys.
3. Configure the Web Server certificate and private key.

After configuration of the above items, reboot the device and the device will come back operate in full approved mode of operation.

10. 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.

11. Mitigation of Other Attack

The module does not mitigate other attack.