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

3e-636M CyberFence Cryptographic Module

HW Version (1.0)
FW Version (5.1)

Security Policy Version 4.0

July 2014

Revision History

Date	Document Version	Description	Author(s)
14-May-2013	1.0	For External Release	Chris Guo
31-Oct-2013	2.0	Revision	Chris Guo
25-Apr-2014	3.0	Revision	Chris Guo
13-June-2014	4.0	Revision	Chris Guo

Table of Contents

1. Introduction

This is a non-proprietary Cryptographic Module Security Policy for the 3e-636M CyberFence Cryptographic Module from 3e Technologies International. This Security Policy describes how the 3e-636M 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. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp

1.1 Cryptographic Module Definition

The 3e-636M Crypto Module primarily acts as a boundary protection device. Using IPSec based VPN technology; it sets up secured channel between a local area network and the wider network. 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 Crypto Module:

Figure 1 – 3e-636M Crypto Module

The critical circuits of the 3e-636M Crypto Module are enclosed in a tamper-resistant opaque metal enclosure, protected by tamper evidence tape intended to provide physical security. There is only one operational mode for the device which is FIPS mode. 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.

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	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

Table 1: Module Security Level

2. Ports & Interfaces

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

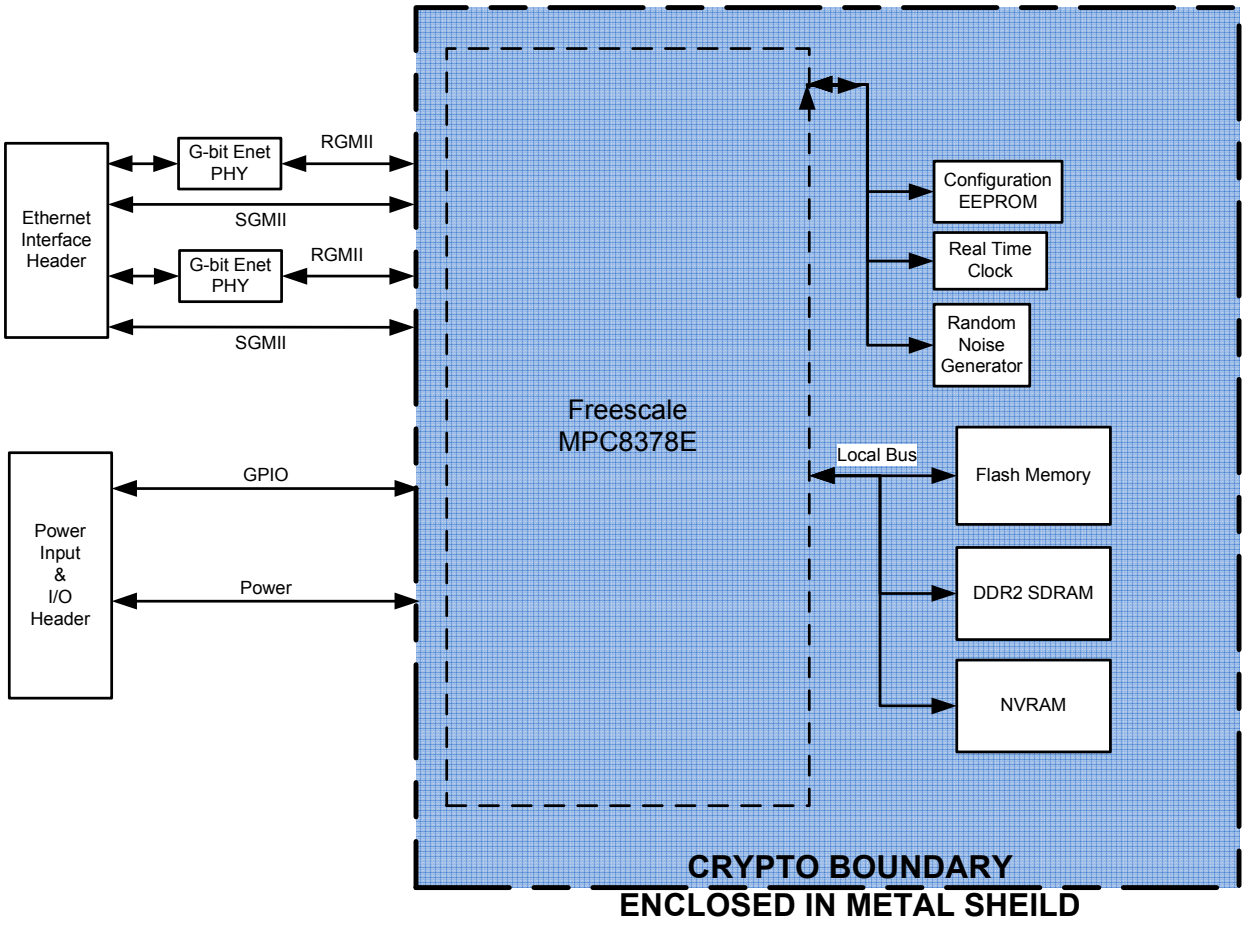

Figure 2 – 3e-636M Crypto Module High Level Block Diagram

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 and RESET pin
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	Username and password	(8-30 chars) Minimum 8 characters => 1:94^8 = 1.641E-16
Administrator	Username and password	(8-30 chars) Minimum 8 characters => 1:94^8 = 1.641E-16
End User	RSA/ ECDSA certificate	2048 and 4096 bits key(RSA), 256/384/521 bits key for ECDSA

Table 2: Identity Based 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).

3.1 End User role

The end user of the device can set up VPN tunnel using IKE v2 to the module and 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 digital certificate and its knowledge of the corresponding private key.

Using conservative estimates and equating a 2048 bit RSA key to a 112 bit symmetric key, or 256 bit ECDSA key equating 128 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 digital certificate and its knowledge of the private key. Per packet integrity check can be optionally turned on by using SHS, AES_CCM or AES_GCM in the IPSec ESP cipher suite.

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 digital certificate and private keys for IPSec, configuration of 801.1X supplicant, 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 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	IKE v2 digital certificate private key, 802.1X supplicant private key, device HTTPS private keys, authentication key with RADIUS server SNMPv3 encryption key	X		
Create and manage Administrator user	Support up to 5 administrator users	X		
Change password	Administrator change his own password only	X	X	
Show system status	View traffic status and systems log excluding security audit log	X	X	
Key zeroization via reboot		X	X	
Factory default	Delete all configurations and set device back to factory default state	X		
Perform Self Test	Run algorithm KAT	X	X	
Load New Firmware	Upload 3eTI digital signed firmware	X		
SNMP Management	All SNMP setting including SNMPv3 encryption key	X	X	
HTTPS Management	Load HTTPS server certificate, private key	X		
IPSec data encryption & decryption				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	IKE v2 digital certificate private key, 802.1X supplicant private key, device HTTPS private keys, authentication key with RADIUS server	Write

Create and manage Administrator user	Administrator Password	Read and Write
Change password	Crypto Officer, 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
Perform Self Test	None	None
IPSec data encryption & decryption	IPSec ESP session keys	Execute
Load new firmware	Firmware signing public key	Read
SNMP management	SNMP 90 bit AES key SNMP Community Name	Read
HTTPS management	HTTPS server certificate, private key	Read

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-636M needs to be added. The current version of the firmware is 5.0. The module uses digital signature to validate the upload firmware. Invalidated 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	
Triple-DES	#1327
AES	#2060
SHS	#1801
RSA	#1072, 1278(1)
HMAC	#1253
ECDSA sign and verify with P256, P384 and P512 curve	#303, 415(2)
RNG	#1076
Component Test (TLS 1.0/1.1/1.2 with SHA-256/SHA-384)	#22
Component Test (ECCDH)	#87

Component Test (IKEv2) #169

The TLS and IKEv2 KDF are CAVP validated, however the TLS and IKEv2 protocol are neither reviewed nor tested by CMVP or CAVP.

Note [1]: RSA signature generation 1024 bit or 1536 bit keys, or with SHA-1, is non-approved according to NIST SP 800-131A.
Note[2]: ECDSA signature generation with SHA-1 is non-approved according to NIST SP 800-131A.

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

Triple-DES	#1329
AES (CCM, CMAC)	#2078
SHS	#1807
HMAC	#1259
AES_GCM	#2105

The product supports the following non-Approved cryptographic algorithms:

- MD5
- NDRNG
- RSA (key wrapping; key establishment methodology between 112 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- Triple-DES (Cert. #1327, key wrapping; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- AES (Cert. #2060, key wrapping; key establishment methodology provides between 128 and 256 bits of encryption strength)
- Diffie-Hellman (CVL Cert. #169, key agreement; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- EC Diffie-Hellman (CVL Cert. #87, key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)

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	Not output	PKCS5 hash in flash	Zeroized when reset to factory	Used to authenticate CO and

		session key)			settings.	Admin role operators
Firmware verification key	ECDSA public key (256 biys)	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
SNMP packet authentication keys, username	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
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**
FIPS ANSI X9.31RNG Seed Key	16-byte value	512 bytes from /dev/urandom file, then hashed by HMAC-SHA256. /dev/urandom is populated by hardware noise generator	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	512 bytes from /dev/urandom file, then hashed by HMAC-SHA256. /dev/urandom is populated by hardware noise generator	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.
IPSec Protocol Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
DH Private Key[1]	1024, 1536, 2048 bits private key	Generated	None	plaintext in RAM	Zeroized when no longer used	IKE v2 SA setup
ECCDH Private Key	256,384,521 bits	Generated	None	Plaintext in RAM	Zeroized when no longer used	IKE v2 SA setup
IPSec SA authentication	RSA (2048,4096)	Input encrypted	Not output	Plaintext in RAM and	Flash copy At factory default	IKE v2 SA authentication

certificate private key	ECDSA (256,384,512)	(using TLS session key)		encrypted in FLASH	RAM copy zeroized when not in use	
IPSec SA private key password	Text string	Input encrypted (using TLS session key)	Not output	Plaintext in RAM and encrypted in FLASH	At factory default	Encrypt the IPSec SA certificate private key
IPSec SA session key	Derived from DH/ECCDH key exchange	Not input	Not output	Plaintext in RAM	Zeroized when no longer used	Encrypt and authenticate SA_Auth messages of IKE v2
IPSec ESP symmetric Data encryption key	AES, AES_CCM, AES_GCM (128,192,256)	Not input (derived from SA setup)	Not output	Plaintext in RAM	Zeroized when child SA lifetime expired	Encrypt IPSec ESP data
3eTI Security Server Keys/CSPs (When Module is configured as 802.1X authenticator)						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
Security Server password	HMAC key (ASCII string)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key", plain text in RAM	Zeroized at factory default reset	Authenticate module to Security Server in support of IPSec SA EAP-TLS authentication
Backend password	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 at factory default reset	Authenticate messages between module and security server in support of IPSec SA EAP-TLS
3eTI 802.1X Supplicant Keys/CSPs (when Module is configured as 802.1X supplicant)						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
802.1X Supplicant private key[2]	RSA (1024,2048,4096) ECDSA (256,384,512)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	Zeroized at factory default reset	Used to authenticate with Authentication Server
802.1X Supplicant private key password	Text string	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 the private key
RFC 2818 HTTPS Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
RSA private key	RSA (2048/3072/4096) (key wrapping; key establishment	Not input (installed at factory)	Not output	Plaintext in flash	Zeroized when new private key is uploaded	Used to support CO and Admin HTTPS interfaces.

	methodology provides 112-150 bits of encryption strength)					
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 a page of the web GUI is served after it is used.	Used to protect HTTPS session.
Public Security Parameter						
HTTPS Public certificate	RSA (2048/3072/4096)	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
HTTPS root certificate	RSA (2048/3072/4096)	Input encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when new root certificate is loaded	Used to setup TLS session for HTTPS
IPSec Public certificate	RSA (2048,4096) ECDSA (256,384,512)	Input encrypted (using TLS session key)	During IPSec SA negotiation	Plaintext in flash	Zeroized when new certificate is loaded	Used for mutual authentication of the IPSec SA
IPSec Root certificate	RSA (2048,4096) ECDSA (256,384,512)	Input encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when new root certificate is loaded	Used for mutual authentication of the IPSec SA
802.1X supplicant public certificate[2]	RSA (1024,2048,4096)	Input encrypted (using TLS session key)	During EAP-TLS session setup	Plaintext in flash	Zeroized when new certificate is loaded	authentication of the EAP-TLS
802.1X supplicant root certificate[2]	RSA (1024,2048,4096)	Input encrypted (using TLS session key)		Plaintext in flash	Zeroized when new root certificate is loaded	authentication of the EAP-TLS

Note[1]: DH with public keys < 2048 or private keys <224 bits is not allowed per NIST SP 800-131A.
Note[2]: RSA key is used for digital signature verification, it's for legacy use per NIST SP 800-131A

7. Self-Tests

The 3e-636M 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
- Triple-DES CBC encrypt KAT

- Triple-DES CBC decrypt KAT
- Triple-DES ECB encrypt KAT
- Triple-DES ECB decrypt KAT
- AES_CCM encrypt KAT
- AES_CCM decrypt KAT
- AES_GCM encrypt KAT
- AES_GCM decrypt KAT
- AES_CMAC KAT
- SHA-1, SHA224, SHA256, SHA384, SHA512 KAT
- HMAC SHA-1, SHA224, SHA256, SHA384, SHA512 KAT

3eTI OpenSSL library Power-on self-tests:

- AES ECB encrypt KAT
- AES ECB decrypt KAT
- Triple-DES CBC encrypt KAT
- Triple-DES CBC decrypt KAT
- HMAC SHA-1, SHA224, SHA256, SHA384, SHA512 KAT
- SHA-1, SHA224, SHA256, SHA384, SHA512 KAT
- ANSI X9.31 RNG KAT
- RSA sign KAT
- RSA verify KAT
- ECDSA sign KAT
- ECDSA verify KAT
- ECCCDH 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 Approved RNG
- Continuous Number Generator Test (CRNGT) on NDRNG
- DH/ECCDH pair-wise consistency test
- Firmware load 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.

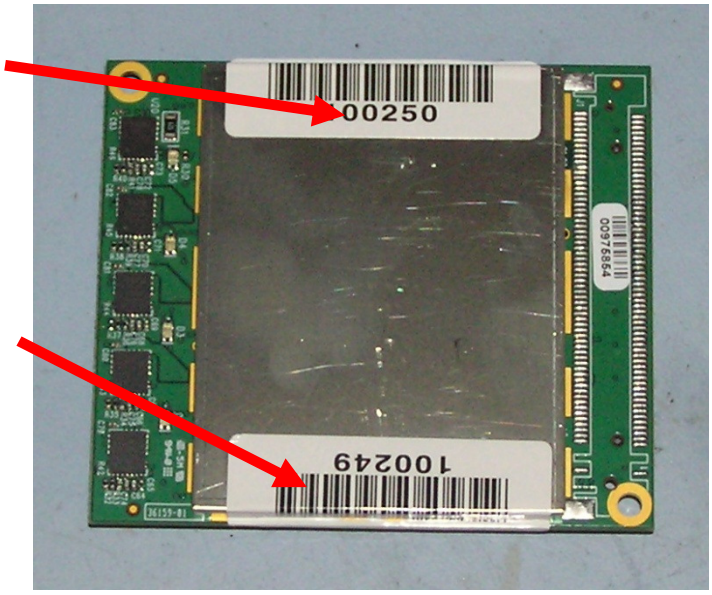

Figure 3 – 3e-636M Crypto Module Tamper Evidence Tape

Tamper evidence tapes are applied to the module at manufacturing time. Crypto Officer is responsible for checking tamper evidence tapes.

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 is larger or equal to 2048 bits if the RSA services are used.

Security Configuration

The module operates in Approved Mode only at all times. 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 Management VPN tunnel with proper CSPs, such as certificate, private key, trust anchor and key expiration time.
3. Configure the Data VPN tunnel with proper CSPs, such as certificate, private key, trust anchor and key expiration time.
4. Configure the 802.1X supplication with proper CSPs, such as certificate, private key and trust anchor. (Optional)

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.