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

3e-636S-1 Accelerated Crypto Module

HW Version 1.0(A)
FW Version 4.3.1

Security Policy Version 1.3

October 2009

Revision History

Date	Document Version	Description	Author(s)
27-Mar-2009	1.0	For external Release	Ryon K. Coleman
08-August	1.1	Update to address comments from CMVP	Chaoxing Lin

Table of Contents

1. Introduction

This document describes the non-proprietary cryptographic module security policy for 3e Technologies International's *3e-636S-1 Accelerated Crypto Module* (Hardware Version: HW V1.0(A); Firmware Version 4.3.1). 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 3e-636S-1 Accelerated Crypto Module meets 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/groups/STM/index.html.

The 3e-636S-1 Accelerated Crypto Module includes an XScale IXP425 processor as a multi-function host processor, network processor, and encryption processor. The XScale contains built-in hardware cryptographic functionality.

Figure 1 below shows the high-level block diagram of the 3e-636S-1 Accelerated Crypto Module:

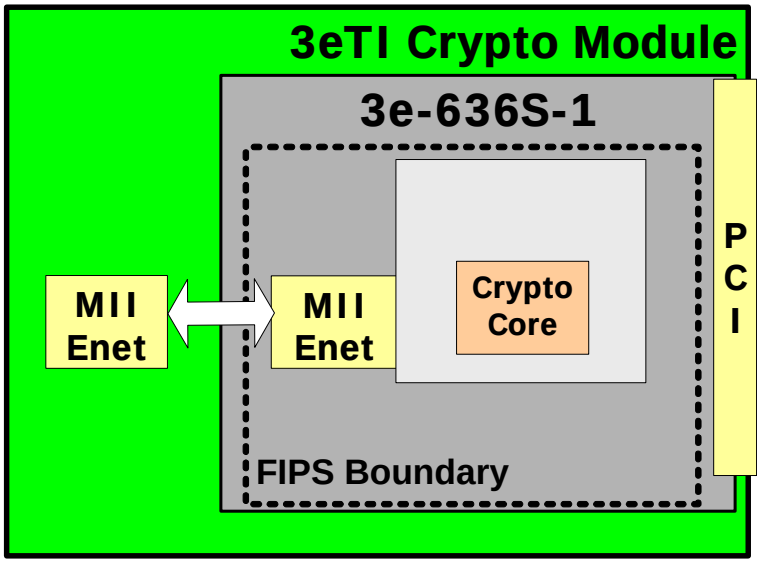

Figure 1 – 3e-636S-1 Accelerated Crypto Module High-Level Block Diagram

The 3e-636S-1 Accelerated Crypto Module will be enclosed in a tamper-resistant opaque metal enclosure, protected by tamper-evident tape intended to provide physical security. This device always runs in FIPS mode.

The components attached to the underside of the PCB and the components (RTC, reset delay chip, logic gates, resistors, underside of chip pads, impedance beads, capacitors) which reside outside of the protective ""can"" of the module are excluded from FIPS requirements.

Secure Configuration & Approved Mode of Operation
The 3e-636S-1 Crypto Officer password must be changed upon 1st-time operation of the 3e-636S-1. Once this secure configuration has been set up, the 3e-636S-1 will be operated in an Approved mode of operation; as long as the device is securely configured (i.e. the Crypto Officer password has been changed from the default value).

Multi-chip Embedded Module
The 3e-636S-1 is a multiple-chip embedded module for the purposes of FIPS 140-2.

2. Ports & Interfaces

The 3e-636S-1 Accelerated Crypto Module contains a very simple set of interfaces, as described below:

a. Status output: Ethernet port pins and I/O connector pins
b. Data output: Ethernet port pins
c. Data input: Ethernet port pins
d. Control input: Ethernet port pins and RESET pin

3. Roles & services

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	Strength of Mechanism
Userid and password	Minimum 8 characters => 94^8 = 1.641E-16
Static Key (Triple-DES or AES)	Triple-DES (192-bits) or AES (128, 192, or 256-bits)

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

The module supports two separate roles.

3.1 End User role

The user of the device can send and receive data to and from the module.
End users can only use the crypto service. The End User is authenticated via implicit knowledge of the pre-shared, symmetric Static Key (AES or Triple-DES). End Users can not configure the device, which must be performed by the Crypto-Officer. They only feed in data packets to be

encrypted, or receive data which has been decrypted. Each successful encryption/decryption of data packets is a successful End User authentication to the module. The peer connects to the device and communicates via an encrypted link using the pre-shared key configured by the Crypto-Officer.

When the device is in End User role, per packet authentication can be optionally turned on by enabling HMAC-SHA1.
When HMAC-SHA1 is selected, an incoming packet on the encrypted port has a 20 byte message digest at the end of the packet. The packet is HMAC-SHA1 rehashed and the result is compared with the 20 byte digest appended to the packet. If they don't match, the packet is dropped. The HMAC-SHA1 key is an additional, optional authentication that can be activated by the Crypto-Officer. However, authentication of the End User is still performed via knowledge of the pre-shared symmetric Static Key.

3.2 Crypto Officer Role:

When a Crypto Officer 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.
Crypto Officer and only Crypto Officer has the privilege to configure the crypto device through web GUI. The Crypto Officer username and password are encrypted and stored inside the crypto boundary.

Crypto Officer and only the Crypto Officer is responsible for performing all configuration for the module. These global configurations include: configuring security functions including entering key information, managing Administrator users, uploading new firmware and bootloader, setting the password policy and performing self-tests on demand, performing system administration, performing zeroization, performing show status, and resetting the module to factory default settings.

The module performs power-on self test on each boot. A reboot command initiated by the Crypto Officer from web GUI is considered a request for system wide self test.

The following table describes the 3e-636S-1 services, including purpose and functions, and the details about the service:

Service and Purpose	Service Inputs	Service Outputs	Authorized Role
Web-based GUI setting of keys and passwords	Control input from the web-based GUI (ie mode setting).	Data output: wired uplink LAN traffic and WLAN traffic	Crypto Officer
Use of all cryptographic functions	Control input from the web-based GUI (ie mode setting). Data input: wired uplink LAN traffic and WLAN traffic	Data output: wired uplink LAN traffic and WLAN traffic	Crypto Officer & End User

4. 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 CryptoLib (User Space Library) Algorithm Implementation 1.0 (RNG only)
RNG: #583

3e Technologies International Inc. 3eTI OpenSSL Algorithm Implementation 0.9.7-beta3
Triple-DES: #783
AES; #1022
SHS: #976
RSA: #490
HMAC: #571

3e Technologies International Inc. 3e-636S-1 Accelerated Crypto Core 1.0
Triple-DES: #784
AES; #1023
SHS: #977
HMAC: #572

The product supports the following non-Approved cryptographic algorithms:
MD5
RSA (key wrapping; key establishment methodology provides 80-bits of encryption strength)

5. Cryptographic Keys and SRDIs

Keys and SRDIs are very rudimentary with the 3e-636S-1 Accelerated Crypto Module. AES ECB key sizes are 128 bits, 192 bits, or 256 bits, as are AES CBC key sizes. Triple-DES ECB key size is 192 bits. Triple-DES CBC key size is 192 bits. HMAC SHA-1 per packet hashing uses a key size of 160 bits. All keys are entered encrypted using **HTTP over TLS** through the HPSSN Module Web GUI.

Below is the Cryptographic Key and Security Relevant Data Item (SRDI) table:

Type	ID	Storage Location	Form	Zeroizable	Zeroization Mechanism	Function
FIPS 186-2 PRNG seed key	Non-approved RNG	RAM	Plaintext	Y	Zeroized every time a new random number is generated using the FIPS PRNG after it is used.	Used to initialize FIPS PRNG

Type	ID	Storage Location	Form	Zeroizable	Zeroization Mechanism	Function
FIPS 186-2 PRNG	FIPS 186-2 PRNG	RAM	Plaintext	Y	Zeroized every time a new random number is generated using the FIPS PRNG after it is used.	Used when a random number is needed
RNG Seed	Non-approved RNG seed	RAM	Plaintext	Y	Zeroized every time a new random number is generated using the FIPS PRNG after it is used.	Used as seed for Non-approved RNG
Static Encryption Keys	AES ECB 128, 192, 256, AES CBC 128, 192, 256, AES CCM 128, Triple-DES ECB, Triple-DES CBC keys	FLASH	Encrypted AES using "system config AES key"	N/A	N/A.	Functional encryption/decryption key
HMAC-SHA-1 key	"HMAC key"	FLASH	Encrypted AES using "system config AES key"	N/A	N/A	Used for keyed per-packet authentication during in-line encryption
Downloaded configuration file password	"downloaded config file passphrase"	RAM	Plaintext	Y	Zeroized when download operation finishes	To protect the configuration file
RSA Private Key	"HTTPS/TLS RSA private key"	FLASH	Plaintext (inaccessible)	Y	Zeroized when firmware is upgraded.	Used in HTTP over TLS for web GUI management
Firmware load key	"Firmware load HMAC key"	FLASH	Plaintext	Y	Zeroized when firmware is upgraded	Used for firmware load message authentication
system config AES key (256 bit)	"system config AES key"	FLASH	Plaintext	Y	Zeroized when firmware is upgraded.	Used to encrypt the configuration file
TLS session key for encryption	"TLS session Triple-DES key"	RAM	Plaintext	Y	Zeroized when a page of the web GUI is served after it is used.	Used to protect HTTPS session.
Crypto Officer password	"CO password"	FLASH	Plaintext	Y	Zeroized when reset to factory settings.	Used to authenticate CO role operators

6. Self-Tests

The 3e-636S-1 Accelerated Crypto Module performs the following power-on self-tests:

OpenSSL Power-on self-tests:

- AES ECB – encrypt/decrypt KAT
- Triple-DES CBC – encrypt/decrypt KAT
- HMAC-SHA-1 KAT
- SHA-1 KAT
- RSA sign/verify test

crypto-1.0 user library Power-on self-tests:

- FIPS 186-2 (Appendix 3.1, 3.3) RNG KAT

Xscale Crypto Engine Power-on self-tests:

- AES ECB & HMAC-SHA1 – (encrypt & hash)/(hash-verify & decrypt) KAT
- AES CBC & HMAC-SHA1 – (encrypt & hash)/(hash-verify & decrypt) KAT
- AES CCM – encrypt/decrypt KAT
- Triple-DES ECB & HMAC-SHA1 – (encrypt & hash)/(hash-verify & decrypt) KAT
- Triple-DES CBC & HMAC-SHA1 – (encrypt & hash)/(hash-verify & decrypt) KAT

Software Integrity Test
- Firmware Integrity Test
- Bootloader Integrity Test

After device is powered on, the first thing done by bootloader is to check firmware integrity. If the integrity is broken, firmware won't boot. Firmware integrity is also performed at POST (Power On Self Test) during firmware boot up. The bootloader integrity is done at POST, too.

Conditional self-tests:
- Continuous Random Number Generator Test (CRNGT) on Approved RNG
- CRNGT on non-Approved RNG

Bypass tests:

Bypass test is not applicable because this crypto module does not provide a bypass mode. By default, the module is in AES-ECB-192 bit encryption mode and all data packets are dropped until a key is configured. Only after Crypto Officer configures the encryption key, data packets will be processed. If LEDs drived by I2C are connected to I2C pins on proprietary IO connector, the "Keyed" LED should be solid green after key is configured.

7. Tamper Evidence

The cryptographic boundary is protected by tamper tape, as shown in the figure below.

Figure 2 – 3e-636S-1 Protected by Tamper Evident Labels

Tamper tapes are applied to the module by manufacturer. Additional labels can be provided to users who integrate this crypto module to their products. These addition labels can be applied on their enclosures for easy checking for tamper evidence. Crypto Officer is responsible for checking tamper tapes.

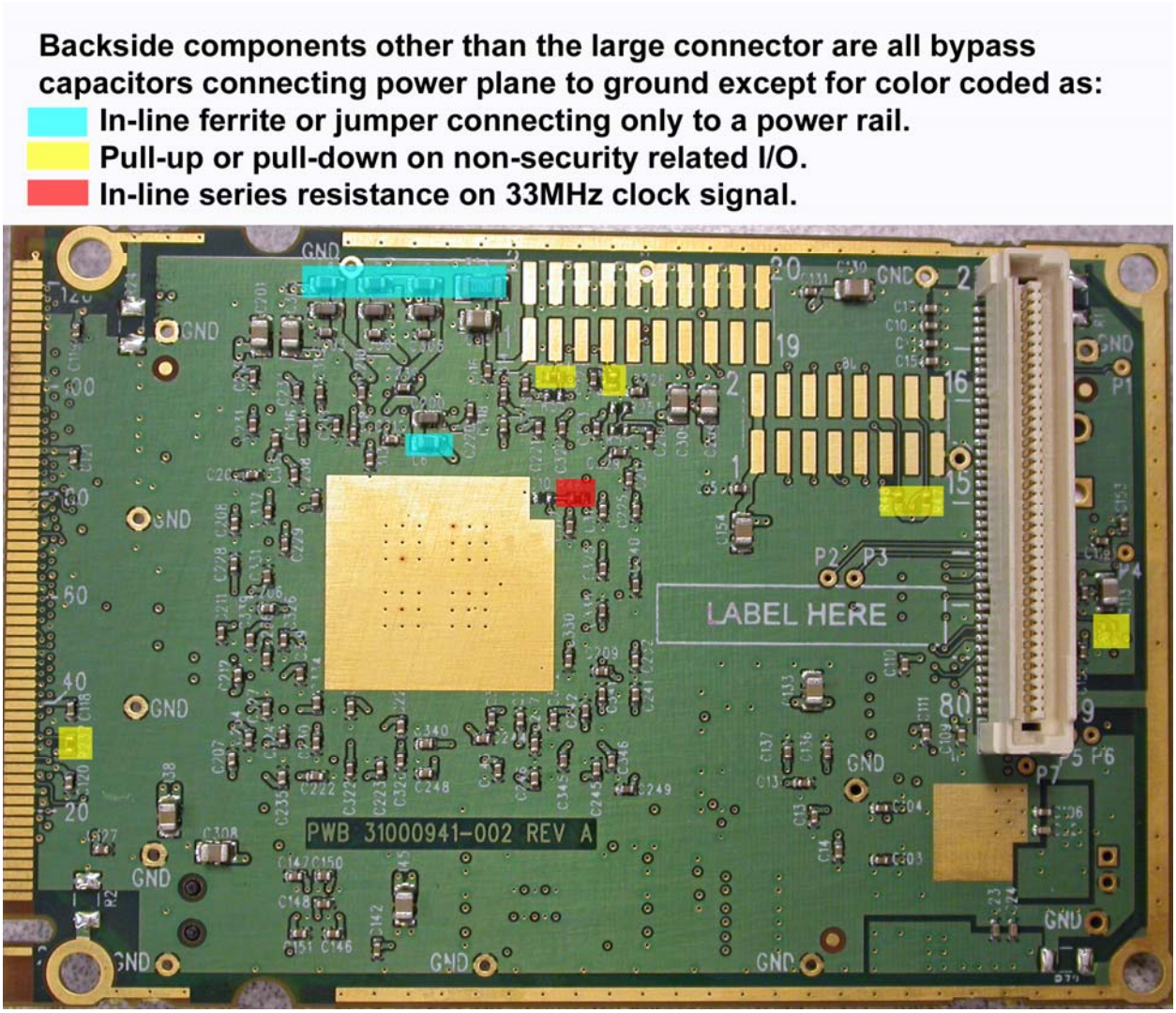

Figure 3 – 3e-636S-1 Backside

Checking for Tamper Evidence

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

Tamper-evident labels may show any of the following as evidence of tampering or removal:

- Label is not preset in the positions prescribed (as shown above)
- Label has been cut
- Label is not stuck down well, or lose
- Adhesive shows outside of label boundary
- Tracking numbers do not match those recorded